# A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

Including examples and a checklist
in form of a project plan

Deliverable WP2006/5.1(CERT-D1/D2)

# Index

**1 Management Summary ........ 2**

**2 Legal Notice ........ 2**

**3 Acknowledgements ........ 2**

**4 Introduction ........ 3**

4.1 TARGET AUDIENCE ........ 4
4.2 HOW TO USE THIS DOCUMENT ........ 4
4.3 CONVENTIONS USED IN THIS DOCUMENT ........ 5

**5 Overall strategy for planning and setting up a CSIRT ........ 6**

5.1 WHAT IS A CSIRT? ........ 6
5.2 POSSIBLE SERVICES THAT A CSIRT CAN DELIVER ........ 10
5.3 ANALYSIS OF THE CONSTITUENCY AND MISSION STATEMENT ........ 12

**6 Developing the Business Plan ........ 18**

6.1 DEFINING THE FINANCIAL MODEL ........ 18
6.2 DEFINING THE ORGANISATIONAL STRUCTURE ........ 20
6.3 HIRING THE RIGHT STAFF ........ 24
6.4 UTILISATION AND EQUIPMENT OF THE OFFICE ........ 26
6.5 DEVELOPING AN INFORMATION SECURITY POLICY ........ 28
6.6 SEARCH FOR COOPERATION BETWEEN OTHER CSIRTS AND POSSIBLE NATIONAL INITIATIVES ........ 29

**7 Promoting the Business Plan ........ 31**

7.1 DESCRIPTION OF BUSINESS PLANS AND MANAGEMENT TRIGGERS ........ 33

**8 Examples of operational and technical procedures (workflows) ........ 36**

8.1 ASSESS THE INSTALLATION BASE OF THE CONSTITUENCY ........ 37
8.2 GENERATING ALERTS, WARNINGS AND ANNOUNCEMENTS ........ 38
8.3 DOING INCIDENT HANDLING ........ 45
8.4 EXAMPLE OF A RESPONSE TIMETABLE ........ 51
8.5 AVAILABLE CSIRT TOOLING ........ 52

**9 CSIRT training ........ 54**

9.1 TRANSITS ........ 54
9.2 CERT/CC ........ 55

**10 Exercise: producing an advisory ........ 56**

**11 Conclusion ........ 61**

**12 Description of the Project Plan ........ 62**

**APPENDIX ........ 64**

A.1 FURTHER READING ........ 64
A.2 CSIRT SERVICES ........ 65
A.3 THE EXAMPLES ........ 74
A.4 SAMPLE MATERIAL FROM CSIRT COURSES ........ 78

# 1 Management Summary

The document at hand describes the process of setting up a Computer Security and Incident Response Team (CSIRT) from all relevant perspectives like business management, process management and technical perspective. This document implements two of the deliverables described in ENISAs Working Programme 2006, chapter 5.1:

- This document: *Written report on step-by-step approach on how to set up a CERT or similar facilities, including examples.*(**CERT-D1**)
- Chapter 12 and external files: *Excerpt of roadmap in itemised form allowing an easy application of the roadmap in practice.* (**CERT-D2**)

# 2 Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external web sites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

# 3 Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special “Thank You” goes to the following contributors:

- Henk Bronk, who as a consultant produced the first version of this document.
- The CERT/CC and especially the CSIRT development team, who contributed most useful material and the sample course material in the annex.
- GovCERT.NL for providing *CERT-in-a-box*
- The TRANSITS team who contributed the sample course material in the annex.
- The colleagues from the Security Policies section in the Technical Department who contributed chapter 6.6
- The countless people who reviewed this document

# 4 Introduction

Communication networks and information systems have become an essential factor in economic and social development. Computing and networking are now becoming ubiquitous utilities in the same way electricity or water supply are.

The security of communication networks and information systems and their availability in particular, is therefore of increasing concern to society. This stems from the risk of problems to key information systems, due to system complexity, accidents, mistakes and attacks to the physical infrastructures that deliver services critical to the well-being of EU citizens.

On 10 March 2004 a European Network and Information Security Agency (ENISA) was established[1]. Its purpose was to ensure a high and effective level of network and information security within the community and to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations within the European Union, thus contributing to the smooth functioning of the internal market.

For several years now a number of security communities in Europe like CERT/CSIRTs, Abuse Teams and WARPs have collaborated for a more secure Internet. ENISA intends to support these communities in their endeavours by providing information about measures for assuring an appropriate level of service quality. Furthermore ENISA intends to enhance its ability to advise the EU member states and the EU bodies in questions of the coverage of specific groups of IT users with appropriate security services. Therefore, building on the findings of the ad-hoc Working Group CERT Cooperation and Support, established in 2005, this new Working Group will deal with questions that relate to the provision of adequate security services (“CERT services”) to specific (categories or groups of) users.

ENISA supports the establishment of new CSIRTs by publishing this ENISA report “*A step-by-step approach on how to set up a CSIRT with a supplementary checklist”, which* will help you establish your own CSIRT.

[1] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. A "European Community agency" is a body set up by the EU to carry out a very specific technical, scientific or management task within the "Community domain" ("first pillar") of the EU.

## *Target audience*

The primary target groups for this report are governmental and other institutions that decide to set up a CSIRT in order to protect their own IT infrastructure or that of their stakeholders.

## *How to use this document*

This document will provide information on what a CSIRT is, what services it can provide and what the necessary steps are to get started. This should give the reader a good and pragmatic overview of the approach, structure and content on how to set up a CSIRT.

Chapter 4 *“Introduction”*
Introduction to this report

Chapter 5 *“Overall strategy for planning and setting up a CSIRT”*
The first section gives a description of what a CSIRT is. It will also provide information about the different environments in which CSIRTs can work and what services they can deliver.

Chapter 6 *“Developing the Business Plan”*
This chapter describes the business management approach to the setting-up process.

Chapter 7 *“Promoting the Business Plan”*
This chapter deal with the business case and funding issues.

Chapter 8 *“Examples of operational and technical procedures”*
This chapter describes the procedure of gaining information and translating it into a security bulletin. This chapter also provides a description of an incident-handling workflow.

Chapter 9 *“CSIRT training”*
This chapter gives a summary of available CSIRT training. For illustration sample course material is provided in the annex.

Chapter 10 *“Exercise: producing an advisory”*
This chapter contains an exercise on how to carry out one of the basic (or core) CSIRT services: the production of a security bulletin (or advisory).

*Chapter 12 “Description of the Project Plan”*
This chapter points to the supplementary project plan (checklist) provided with this guide. This plan aims at being a simple to use tool for the implementation of this guide.

## *Conventions used in this document*

To give guidance to the reader, each chapter starts with a summary of the steps taken so far in the process of setting up a CSIRT. These summaries are outlined in boxes like the following:

> We have taken the first step

Each chapter will conclude with a practical example of the steps discussed. In this document the “Fictitious CSIRT” will be a small independent CSIRT for a medium-sized company or institution. A summary can be found in the appendix.

> **Fictitious CSIRT**

# 5 Overall strategy for planning and setting up a CSIRT

For a successful start of the process of setting up a CSIRT it is important to have a clear vision of the possible services the team can provide to its customers, in the “CSIRT world” better known as ‘constituents’. Therefore it is necessary to understand what the constituents needs are to provide the appropriate services in the appropriate timeliness and quality.

## *What is a CSIRT?*

CSIRT stands for Computer Security Incident Response Team. The term CSIRT is used predominantly in Europe for the protected term CERT, which is registered in the USA by the CERT Coordination Center (CERT/CC).
There exist various abbreviations used for the same sort of teams:

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

The first major outbreak of a worm in the global IT infrastructure occurred in the late 1980s. The worm was named Morris[2] and it spread swiftly, effectively infecting a great number of IT systems around the world.

This incident acted as a wake-up call: suddenly people got aware of a strong need for cooperation and coordination between system administrators and IT managers in order to deal with cases like this. Due to the fact that time was a critical factor, a more organised and structural approach on handling IT security incidents had to be established. And so a few days after the “Morris-incident” the Defence Advanced Research Projects Agency (DARPA) established the first CSIRT: the CERT Coordination Center (CERT/CC[3]), located at the Carnegie Mellon University in Pittsburgh (Pennsylvania).

This model was soon adopted within Europe, and 1992 the Dutch Academic provider SURFnet launched the first CSIRT in Europe, named SURFnet-CERT[4]. Many teams followed and at present ENISAs *Inventory of CERT activities in Europe*[5] lists more than 100 known teams located in Europe.

Over the years CERTs extended their capacities from being a mere reaction force to a complete security service provider, including preventative services such as alerts, security advisories, training and security management services. The term “CERT” was soon considered insufficient. As a result, the new term “CSIRT” was established at the

[2] More info about the Morris Worm http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC, http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

[5] ENISA Inventory http://www.enisa.europa.eu/cert_inventory/

end of the1990s. At the moment both terms (CERT and CSIRT) are used synonymously, with CSIRT being the more precise term.

## 5..1 The term *Constituency*

From now on the (in the CSIRT communities) well established term ‘constituency’ will be used to refer to the customer base of a CSIRT. A single customer will be addressed as ‘constituent’, a group as ‘constituents’.

## 5..2 Definition of a CSIRT

A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches.

In order to mitigate risks and minimise the number of required responses, most CSIRTs also provide preventative and educational services for their constituency. They issue advisories on vulnerabilities in the soft and hardware in use, and also inform the users about exploits and viruses taking advantage of these flaws. So the constituents can quickly patch and update their systems. See chapter *5.2 Possible services* for a complete list of possible services.

## 5..3 The benefits of having a CSIRT

Having a dedicated IT security team helps an organisation to mitigate and prevent major incidents and helps to protect its valuable assets.

Further possible benefits are:

- Having a centralised coordination for IT security issues within the organisation (Point of Contact, PoC).
- Centralised and specialised handling of and response to IT incidents.
- Having the expertise at hand to support and assist the users to quickly recover from security incidents.
- Dealing with legal issues and preserving evidence in the event of a lawsuit.
- Keeping track of developments in the security field.
- Stimulating cooperation within the constituency on IT security (awareness building).

**Fictitious CSIRT (step 0)**

**Understanding what a CSIRT is:**

The sample CSIRT will have to serve a medium institution made up of 200 staff members. The institution has its own IT department and two other branch offices in the same country. IT plays a key roll for the company because it’s used for internal communication, data network and a 24x7 e-business. The institution has its own network and disposes of a redundant connection to the internet via two different ISPs.

## 5..4 Description of the different kinds of CSIRT environments

We have taken the first step

1. Understanding what a CSIRT is and what benefits it might provide.

>> The next step is to answer the question: "To what sector will CSIRT services be delivered to?"

When starting up a CSIRT (just like any other business) it is very important to very soon develop a clear view on who the constituents are and what kind of environment the CSIRT services will be developed for. At this moment we distinguish the following 'sectors', listed alphabetically:

- Academic Sector CSIRT
- Commercial CSIRT
- CIP/CIIP Sector CSIRT
- Governmental Sector CSIRT
- Internal CSIRT
- Military Sector CSIRT
- National CSIRT
- Small & Medium Enterprises (SME) Sector CSIRT
- Vendor CSIRT

**Academic Sector CSIRT**

*Focus*

An academic sector CSIRT provides CSIRT services to academic and educational institutions, such as universities or research facilities, and their campus Internet environments.

*Constituents*

Typical constituents of this type of CSIRT are staff and students of universities.

**Commercial CSIRT**

*Focus*

A commercial CSIRT provides CSIRT services commercially to their constituents. In the case of an ISP the CSIRT mostly provides abuse services to end-user customers (Dial-in, ADSL) and CSIRT services to their professional customers.

*Constituents*

Commercial CSIRTs usually deliver their services to constituents who pay for them.

**CIP/CIIP Sector CSIRT**

*Focus*

CSIRTs in that sector mainly focus on Critical Information Protection and / or Critical Information and Infrastructure protection. In most cases this specialised CSIRT cooperates closely with a Governmental CIIP department. It covers all critical IT sectors in the country and protects that country's citizens.

*Constituents*

Government; critical IT businesses; citizens

**Governmental Sector CSIRT**

*Focus*

A governmental CSIRT provides services to government agencies and in some countries to the citizens.

*Constituents*

Government and governmental related agencies; in some countries alerting services are also provided to the citizens (for example in Belgium, Hungary, The Netherlands, United Kingdom or Germany).

**Internal CSIRT**

*Focus*

An internal CSIRT provides services to its hosting organisation only. This describes more the functioning rather than a sector. A lot of telecommunication organisations and banks for example run their own internal CSIRTs. They usually do not maintain a website for the public.

*Constituents*

Internal staff and IT department of the hosting organisation

**Military Sector CSIRT**

*Focus*

A CSIRT in that sector provides services to military organisations with responsibilities for IT infrastructure that is needed for defence purposes.

*Constituents*

Staff of military institutions or closely related entities, for example the Department of Defence

**National CSIRT**

*Focus*

A CSIRT with a national focus, considered as security point of contact for a country. In some cases the governmental CISRT also acts as national PoC (like UNIRAS in the UK).

*Constituents*

This type of CSIRT usually does not have direct constituents, as the national CSIRT only plays an intermediary role for the whole country

**Small & Medium Enterprises (SME) Sector CSIRT**

*Focus*

A self organised CSIRT that provides its services to its own business branch or similar user group.

*Constituents*

Constituents of these CSIRTs might be SMEs and their staff, or special interest groups like the "Association of Towns and Municipalities" of a country.

**Vendor CSIRT**

*Focus*

A vendor CSIRT focuses on the support of the vendor-specific products. Its aim usually is to develop and provide solutions in order to remove vulnerabilities and to mitigate potential negative effects of flaws.

*Constituents*

Product owners

As described in the paragraph about national CSIRTS, it is possible that a team serves more than one sector. This has an impact for example on the analysis of the constituency and its needs.

**Fictitious CSIRT (step 1)**

**Starting phase**

In the starting phase the new CSIRT is planned as an Internal CSIRT, providing its services for the hosting company, the local IT department and the staff. It also supports and coordinates the handling of IT security related incidents between the different branch offices.

## Possible services that a CSIRT can deliver

We have taken the first two steps

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?

>> The next step is to answer the question, w*hat services to provide to the constituents.*

There are many services that a CSIRT can deliver, but so far no existing CSIRT provides all of them. So the selection of the appropriate set of services is a crucial decision. Below you will find a short overview of all known CSIRT services, as defined in the "Handbook for CSIRTs" published by the CERT/CC[6].

[6] CERT/CC CSIRT handbook http://www.cert.org/archive/pdf/csirt-handbook.pdf

| **Reactive Services** | **Proactive Services** | **Artifact Handling** |
|---|---|---|
| • **Alerts and Warnings**<br>• **Incident Handling**<br>• **Incident analysis**<br>• **Incident response support**<br>• **Incident response coordination**<br>• Incident response on site<br>• Vulnerability Handling<br>• Vulnerability analysis<br>• Vulnerability response<br>• Vulnerability response coordination | • **Announcements**<br>• Technology Watch<br>• Security Audits or Assessments<br>• Configuration and Maintenance of Security<br>• Development of Security Tools<br>• Intrusion Detection Services<br>• Security-Related Information Dissemination | • *Artifact analysis*<br>• *Artifact response*<br>• *Artifact response coordination* |
| | | ***Security Quality Management*** |
| | | • *Risk Analysis*<br>• *Business Continuity and Disaster Recovery*<br>• *Security Consulting*<br>• *Awareness Building*<br>• *Education/Training*<br>• *Product Evaluation or Certification* |

*Fig. 1 CSIRT Services list from CERT/CC*[7]

**The core services (marked in bold letters)**: there is a distinction made between reactive and proactive services. Proactive services aim at prevention of incidents through awareness building and training, while reactive services aim at handling incidents and mitigating the resulting damage.

**Artifact handling** contains the analysis of any file or object found on a system that might be involved in malicious actions, like leftovers from viruses, worms, scripts, trojans, etc. It also contains the handling and distribution of resulting information to vendors and other interested parties, in order to prevent further spreading of malware and to mitigate the risks.

**Security and Quality management services** are services with longer term goals and include consultancy and educational measures.

See the appendix for a detailed explanation of CSIRT services.

Choosing the right services for your constituents is an important step and will be further referred to in the chapter *6.1 Defining the Financial Model*.

Most CSIRTs start with distributing ‘Alerts and Warnings’, make ‘Announcements’ and providing ‘Incident Handling’ for their constituents. These core-services usually give a good profile and attention value with the constituency, and are mainly considered as real “added value”.

A good practice is to start with a small group of ‘pilot’-constituents, deliver the core-services for a pilot-period of time and request feedback afterwards.

[7] CSIRT Services list from CERT/CC: http://www.cert.org/csirts/services.html

Interested pilot-users usually provide constructive feedback and help to develop tailor-made services.

**Fictitious CSIRT (step 2)**

**Choosing the right services**

In the starting phase it is decided that the new CSIRT will focus mainly on providing some of the core-services for the employees.

It's decided that after a pilot-phase the extension of the service portfolio might be considered and some 'Security Management Services' might be added. That decision will be made based on the feedback from the pilot-constituents and in close cooperation with the Quality Assurance department.

## *Analysis of the constituency and mission statement*

We have taken the first three steps:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.

>> The next step is to answer the question, *what kind of approach should be chosen to start up the CSIRT?*

The next step is a deeper look into the constituency with the main goal to choose the correct communication channels:

- Defining the communication approach to the constituents
- Defining the mission statement
- Making a realistic implementation/project plan
- Defining the CSIRT services
- Defining the organisational structure
- Defining the Information Security policy
- Hiring the right staff
- Utilisation of your CSIRT office
- Looking for cooperation between other CSIRTs and possible national initiatives

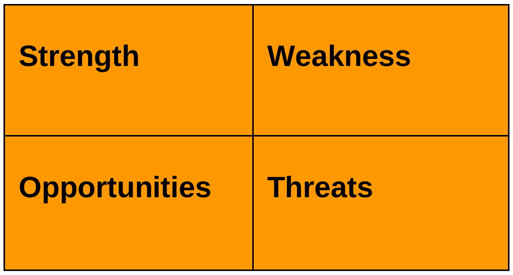
These steps will be described more in detail in the following paragraphs and can be used as input for the business- and the project plan.

## 5..1 Communication approach to the constituency

As said before it's very important to know the needs of the constituency as well as your own strategy of communication, including the communication channels that are most appropriate to approach them with information.

Management theory knows several possible approaches to this problem of analysing a target group. In this document we describe two of them: the SWOT- and the PEST-analysis.

**SWOT analysis**
A SWOT Analysis is a strategic planning tool used to evaluate the **S**trengths, **W**eaknesses, **O**pportunities, and **T**hreats involved in a project or in a business venture or in any other situation requiring a decision. The technique is credited to Albert Humphrey, who led a research project at Stanford University in the 1960s and '70s, using data from the Fortune 500 companies.[8]



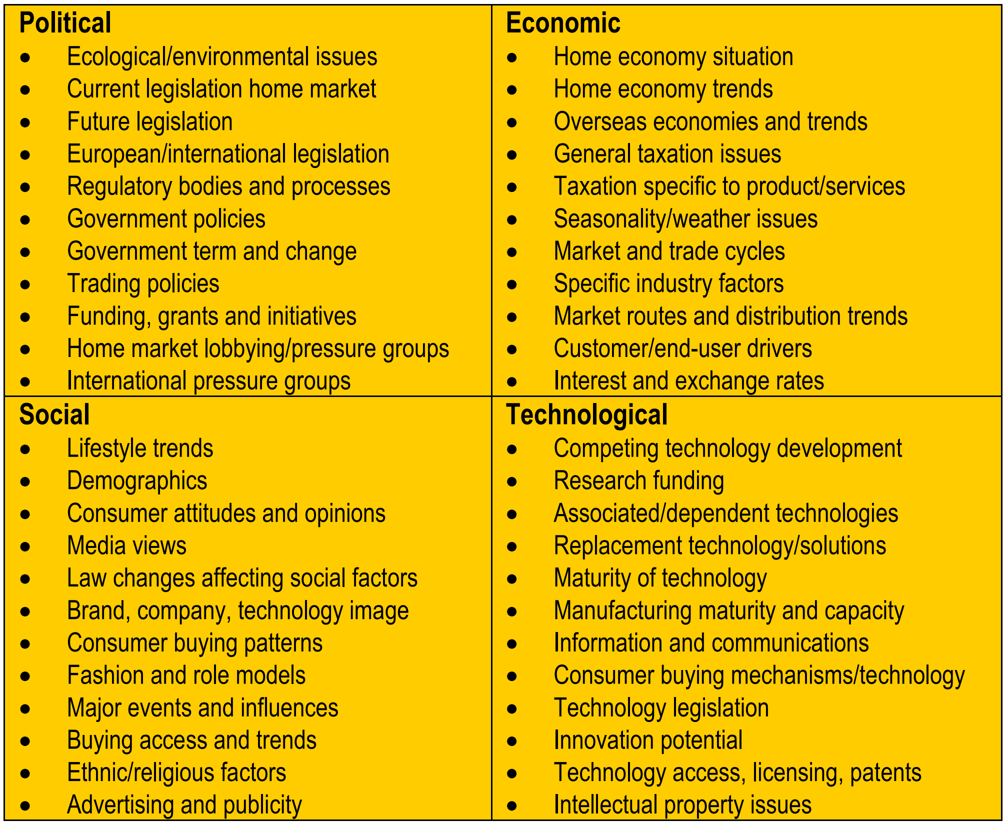
| | |
|---|---|
| **Strength** | **Weakness** |
| **Opportunities** | **Threats** |

*Fig. 2SWOT analysis*

[8] SWOT analysis at Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

### PEST analysis

The PEST analysis is another important and widely used tool to analyse the constituency with the goal to understand **P**olitical, **E**conomic, **S**ocio-cultural and **T**echnological circumstances of the environment a CSIRT is operating in. It will help to determine whether the planning is still in tune with the environment and probably helps to avoid actions taken out of wrong assumptions.



| **Political** | **Economic** |
|---|---|
| • Ecological/environmental issues | • Home economy situation |
| • Current legislation home market | • Home economy trends |
| • Future legislation | • Overseas economies and trends |
| • European/international legislation | • General taxation issues |
| • Regulatory bodies and processes | • Taxation specific to product/services |
| • Government policies | • Seasonality/weather issues |
| • Government term and change | • Market and trade cycles |
| • Trading policies | • Specific industry factors |
| • Funding, grants and initiatives | • Market routes and distribution trends |
| • Home market lobbying/pressure groups | • Customer/end-user drivers |
| • International pressure groups | • Interest and exchange rates |
| **Social** | **Technological** |
| • Lifestyle trends | • Competing technology development |
| • Demographics | • Research funding |
| • Consumer attitudes and opinions | • Associated/dependent technologies |
| • Media views | • Replacement technology/solutions |
| • Law changes affecting social factors | • Maturity of technology |
| • Brand, company, technology image | • Manufacturing maturity and capacity |
| • Consumer buying patterns | • Information and communications |
| • Fashion and role models | • Consumer buying mechanisms/technology |
| • Major events and influences | • Technology legislation |
| • Buying access and trends | • Innovation potential |
| • Ethnic/religious factors | • Technology access, licensing, patents |
| • Advertising and publicity | • Intellectual property issues |

*Fig. 3 Pest analysis model*

A detailed description of the PEST analysis can be found in Wikipedia[9].

Both tools give a comprehensive and structured overview of what the need of the constituents are. The results will complement the business proposal and by this help to obtain funding for the setting up of the CSIRT.

### Communication channels

An important topic to include in the analysis is possible communication and information distribution methods ("How to communicate with the constituency?")

If possible regular personal visits of the constituents should be considered. It's a proven fact that face-to face-meetings ease cooperation. If both sides are willing to work together these meetings will lead to a more open relationship.

[9] PEST analysis at Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Usually CSIRTs operate a set of communication channels. The following proved useful in practice and are worth to consider

- Public website
- Closed member area on the website
- Web-forms to report incidents
- Mailing lists
- Personalised e-mail
- Phone / Fax
- SMS
- 'Old fashioned' paper letters
- Monthly or annual reports

Besides using e-mail, web-forms, phone or fax to facilitate incident handling (to receive incident reports from the constituency, coordinate with other teams or give feedback and support to the victim) most CSIRTs publish their security advisories on a publicly available website and via a mailing lists.

**!** If possible, information should be distributed in a secure manner. E-mail for example can be digitally signed with PGP, and sensitive incident data should always be sent encrypted.

For more information see the chapter *8.5 Available CSIRT Tooling*. See also chapter *2.3* of the *RFC2350*[10].

**Fictitious CSIRT (step 3a)**

**Making an analysis of the constituency and the appropriate communication channels**

A brainstorming session with some key persons from management and the constituency generated enough input for a SWOT analysis. This lead to the conclusion that there is a need for the core-services:

- Alerts and warnings
- Incident handling (analysis, response support and response coordination)
- Announcements

It must be ensured that the information is distributed in a well-organised manner to reach a biggest possible part of the constituency. So the decision is made that alerts, warnings and announcements in the form of security advisories will be published on a dedicated website and distributed via a mailing list. The CSIRT facilitates e-mail, phone and fax for receiving of incident reports. A unified web-form is planned for the next step.

See next page for a sample SWOT analysis.

[10] http://www.ietf.org/rfc/rfc2350.txt

| | |
|---|---|
| **Strength**<br>• There is some knowledge within the company.<br>• They like the plan and are willing to cooperate<br>• Support and funding by the mgt. board | **Weakness**<br>• Not much communication between the different departments and branch offices.<br>• No coordination with IT incidents<br>• Lots of ‘little departments” |
| **Opportunities**<br>• Huge flood of non-structured vulnerability information<br>• Strong need for coordination<br>• Reducing losses due to incidents<br>• Lot of open ends on the matter of IT security<br>• Educating staff on IT security | **Threats**<br>• Not much money available<br>• Not much staffing<br>• High expectations<br>• Culture |

*Fig. 4 Sample SWOT analysis*

## 5..2 Mission statement

After analysing the constituency needs and wishes concerning CSIRT services the next step should be the drafting of a mission statement.

A mission statement describes the organisations basic function in society, in terms of the products and services it provides for its constituents. It allows communicating clearly the existence and the function of the new CSIRT.

It’s a good practice to make the mission statement compact but not too tight, because usually it will stay invariant for a couple of years.

Here are some examples for mission statements from operating CSIRTs:

*“<Name of CSIRT> provides information and assistance to its <constituents (define your constituents)> in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur.”*

*"To offer support to <Constituents> on the prevention of and response to IT related Security Incidents"*[11]

[11] Mission statement of Govcert.nl: http://www.govcert.nl

The mission statement is a very important and necessary step to start with. Please refer to chapter *2.1* of *RFC2350*[12] for a more detailed description of what information a CSIRT should publish.

| **Fictitious CSIRT (step 3b)** |
|---|
| The management of the fictitious CSIRT has made the following mission statement:<br>*"Fictitious CSIRT provides information and assistance to the staff of its hosting company to reduce the risks of computer security incidents as well as responding to such incidents when they occur."*<br><br>By this fictitious CSIRT makes clear that it is an internal CSIRT and that its core business is to deal with IT security related issues. |

[12] http://www.ietf.org/rfc/rfc2350.txt

# 6 Developing the Business Plan

We have taken the following steps:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents
5. Defining the mission statement

>> The next step is to define the business plan

The output from the analysis gives you a good overview of the needs and the (assumed) weaknesses of the constituency, so it is taken as input for the next step.

### *Defining the financial model*

After the analysis a couple of core-services were picked to start with. The next step is to think about the financial model: what parameters of service provision are both suitable and payable.

In a perfect world the funding would be adapted to the needs of the constituency, but in reality the portfolio of services that can be provided must adapt to a given budget. So it's more realistic to start with the planning of monetary issues.

## 6..1 Cost model

The two main factors that influence the costs are the determination of service hours and the number (and quality) of staff to be employed. Is there a need for delivering 24x7 incident response and technical support or will these services only be provided during office hours?

Depending on the desired availability and the office equipment (is it for example possible to work from home?) it can be beneficial to work with an on-call duty roster or a scheduled duty roster.

A thinkable scenario is to deliver both proactive and reactive services during office hours. Outside office hours only limited services will be provided, for example in the case of major disasters and incidents only, by a staff member on call-duty.

Another option is to look for international cooperation between other CSIRT teams. There are already examples of functioning “Following the Sun” cooperation. For example cooperation between European and American teams proved to be beneficial and provide a good way to share each others capacity. Sun Microsystems CSIRT for example, who have multiple branch offices in different time zones around the world (but all are members of the same CSIRT team) realise 24x7 services by constantly shift duties among the teams around the globe. This does limit the costs, because teams always only work during normal office hours and also provide services for the “sleeping part” of the world.

It is good practice to especially analyse the need for 24x7 services deeply with the constituency. Alerts and Warnings provided during night times do not make much sense when the recipient will only read it the next morning. There is a fine line between “needing a service” and “wanting a service”, but especially the working hours make a huge difference in the number of staff and the needed facilities, and by this have a major impact on the cost model.

## 6..2 Revenue model

When knowing the cost it’s a good next step to think about possible revenue models: how can the planned services be financed. Here are some possible scenarios to evaluate:

**Use of existing resources**

It’s always beneficial to assess the already present resources in other parts of the company. Is there already suitable staff employed (for example in the existing IT department) with the needed background and expertise? Probably arrangements can be found with the management to second this staff to the CSIRT for the starting phase, or they provide support for the CSIRT on an ad-hoc basis.

**Membership fee**

Another possibility is to sell your services to the constituency, by an annual/quarterly membership fee. Additional services could be paid for on a per-use basis, for example consultancy services or security audits.

Another thinkable scenario: services for the (internal) constituency are provided for free, but services delivered to external customers may have to be paid for. Another idea is to publish advisories and information bulletins on the public website and have a “Members Only” section with special, more detailed or tailored information.

It has been proven in the practice that “Subscription per CSIRT service” has only a limited use for providing enough funding, especially in the start-up phase. There are for example fixed basic costs for the team and equipment that have to be paid for in advance. The funding of these costs by selling CSIRT services is difficult and requires a very detailed financial analysis to find the “break-even point”.

**Subsidy**

Another possibility worth to consider might be to apply for project subsidy provided from the government or a governmental body, as nowadays most countries have funds available for IT security projects. Contacting the Ministry of the Interior might be a good start.

A mixture of different venue models is of course possible.

## *Defining the organisational structure*

The suitable organisational structure of a CSIRT depends highly on the existing structure of the hosting organisation and the constituency. It also depends on the accessibility of skilled experts to be hired permanently or on an ad-hoc basis.

A typical CSIRT defines the following roles within the team:

**General**

- General manager

**Staff**

- Office manager
- Accountant
- Communication consultant
- Legal consultant

**Operational Technical team**

- Technical team leader
- Technical CSIRT technicians, delivering the CSIRT services
- Researchers

**External consultants**

- Hired when needed

It is extremely helpful to have a legal specialist on board especially during the starting phase of the CSIRT. It will raise the cost but at the end of the day will save time and legal troubles.

Depending on the variety of expertise inside the constituency, and also when the CSIRT has a high media profile, it proved very useful to also have a communication expert in the team. These experts can focus on translating difficult technical issues to more understandable messages for the constituents or media-partners. The communication expert also will provide feedback from the constituency to the technical experts, so he/she might act as a “translator” and “facilitator” between these two groups.

Following are a few examples of organisational models in use by operational CSIRTs.

## 6..1 The independent business model

The CSIRT is rolled out and acts as an independent organisation, with its own management and employees.

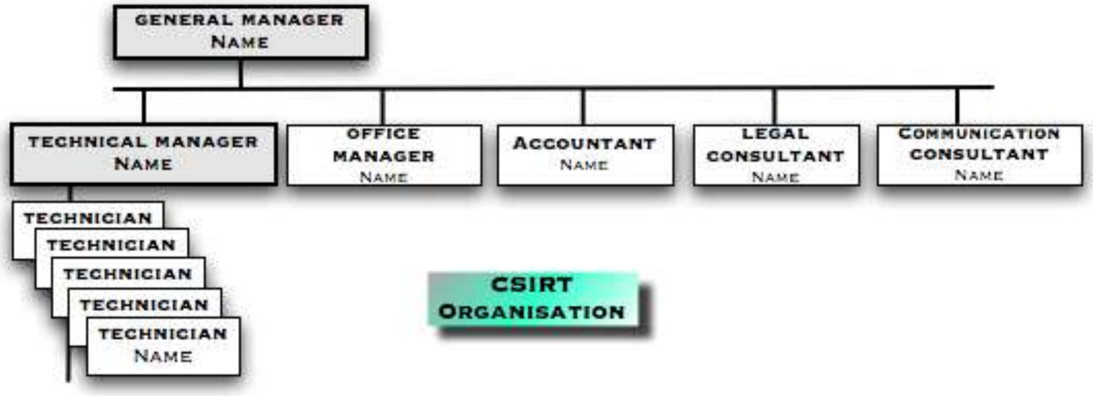


*Fig. 5 Independent Business model*

## 6..2 The embedded model

This model can be used if a CSIRT is to be established within an existing organisation, using an existing IT department for example. The CSIRT is headed up by a team leader and he or she is responsible for the CSIRT activities. The team leader gathers the necessary technicians when solving incidents or working on CSIRT activities. He or she can request assistance within the existing organisation for specialist support.

This model can also be adapted for specific situations as they arise. In this case, the team has a fixed number or Full Time Equivalent (FTE) allocated. The abuse desk at an ISP, for example, is certainly a fulltime job for one or (in most cases) more than one FTE.

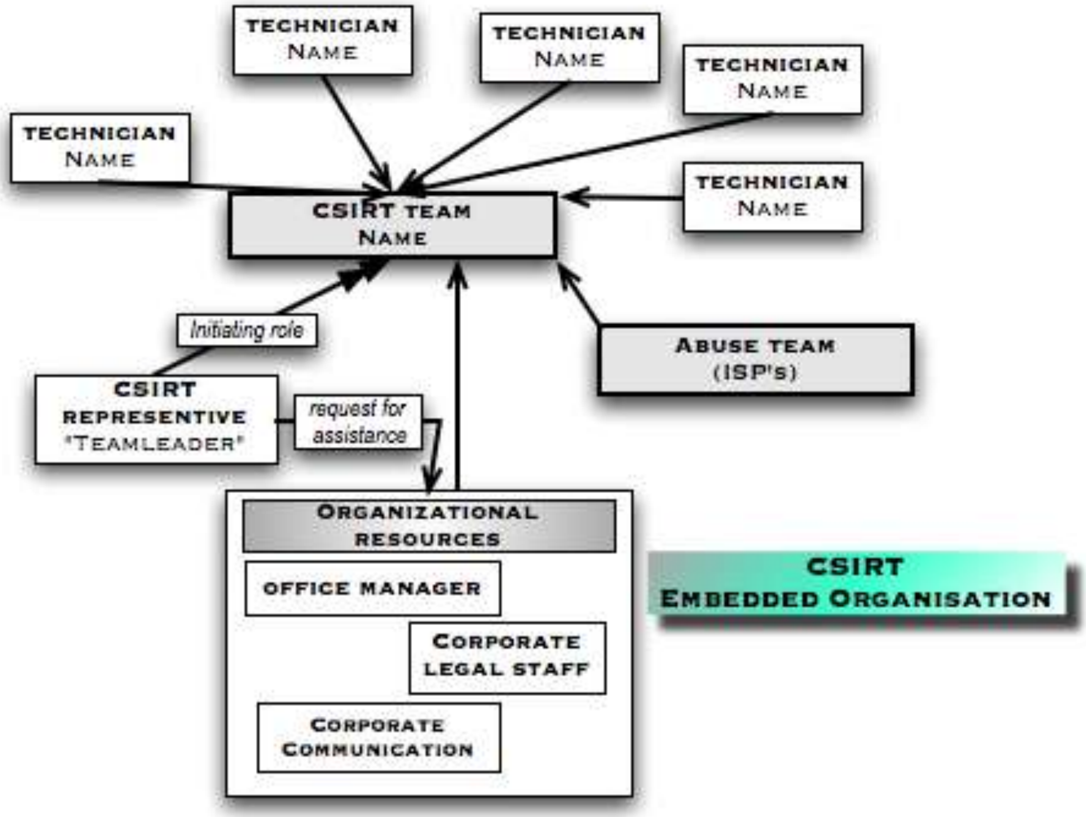


*Fig. 6 Organisational embedded model*

## 6..3 The campus model

The campus model, as the name suggests, is adopted mostly by academic and research CSIRTs. Most academic and research organisations are comprised of various universities and campus facilities at different locations, spread over a region or even the whole country (like in the case of the NRENs, the National Research Networks). Usually these organisations are independent from each other, and they often run their own CSIRT. These CSIRTs are usually organised under the umbrella of the 'mother' or core CSIRT. The core CSIRT coordinates and is the single point of contact for the outside world. In most cases the core CSIRT will also provide the core CSIRT services as well as distributing incident information to the appropriate campus CSIRT.

Some CSIRTs circulate their CSIRT core services with the other campus CSIRTs, which results in lower overhead for the Core CSIRT.

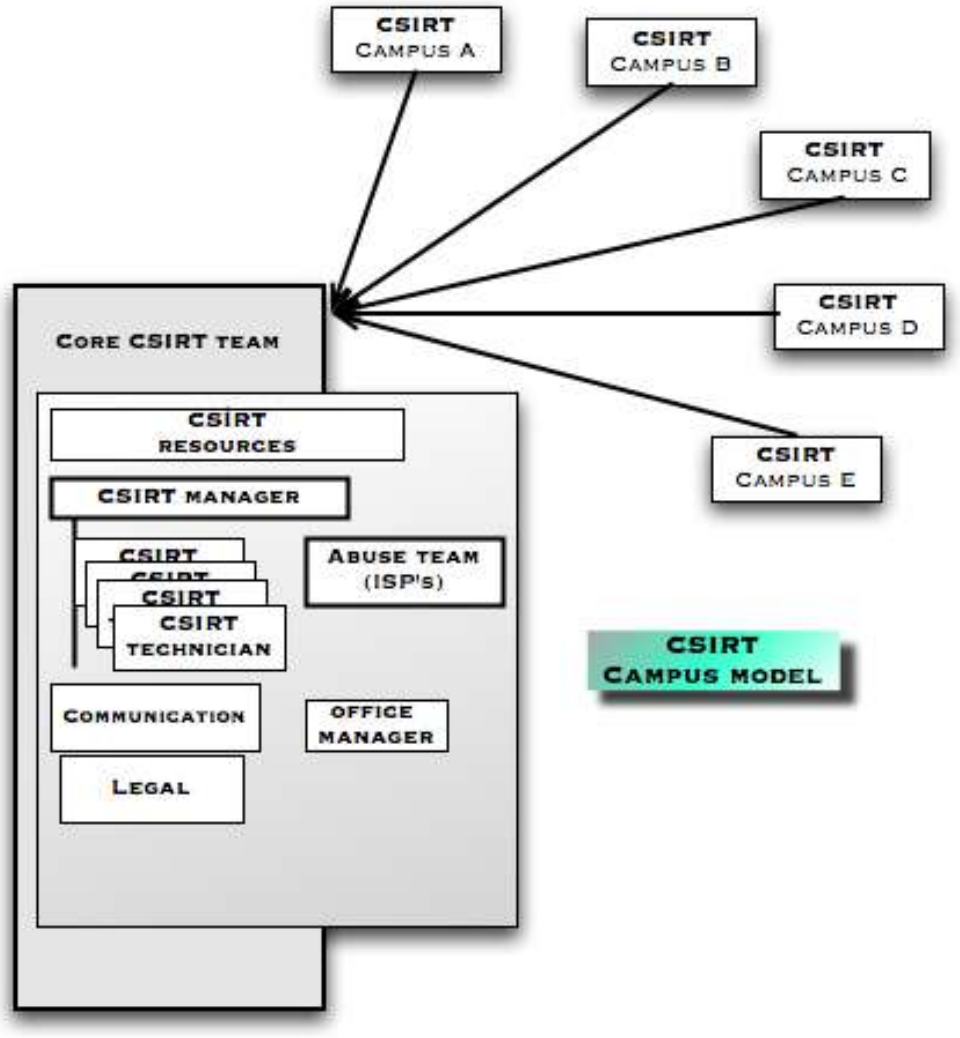


*Fig. 7 Campus model*

## 6..4 The voluntary model

This organisational model describes a group of people (specialists) that join together to provide advice and support to each other (and others) on a voluntary basis. It's a loosely fitted community and is highly dependant on the motivation of the participants.

This model is for example adopted by the WARP community[13].

### *Hiring the right staff*

Having decided on the services and the level of support to be delivered, and after choosing an organisational model, the next step is to find the right amount of skilled people for the job.

It's nearly impossible to provide hard figures on the amount of technical staff needed from this perspective, but the following key values have proven to be a good approach:

- In order to deliver two core services of the distribution of advisory bulletins as well as incident handling: a minimum of **4** FTE.

- For a full service CSIRT during office hours, and maintaining systems: a minimum of **6 to 8** FTE.

- For a fully staffed 24x7 shift (2 shifts during out-of-office hours), the minimum is about **12** FTE.

These numbers also include redundancies for cases of sickness, holidays, etc. It's also necessary to check the local collective labour agreements. If people work outside office hours this might result in extra costs in form of extra allowance that have to be paid.

[13] The WARP initiative http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Following a brief overview of key competencies for the technical experts for a CSIRT

**General technical staff job description items:**

**Personal competences**

- Flexible, creative and a good team spirit
- Strong analytical skills
- Ability to explain difficult technical matters in easy wording
- A good feeling for confidentiality and working in a procedural matter
- Good organisational skills
- Stress durable
- Strong communicative and writing skills
- Open minded and willing to learn

**Technical competences**

- Broad knowledge of internet technology and protocols
- Knowledge of Linux and Unix systems (depending on the equipment of the constituency)
- Knowledge of Windows systems (depending on the equipment of the constituency)
- Knowledge of network infrastructure equipment (Router, switches, DNS, Proxy, Mail, etc.)
- Knowledge of Internet applications (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Knowledge of Security threats (DDoS, Phishing, Defacing, sniffing, etc.)
- Knowledge of risk assessment and practical implementations

**Additional competencies**

- Willing to work 24x7 or on call duty (depending on the service model)
- Maximum of travelling distance (in case of emergency availability in the office; maximum travelling time)
- Level of education
- Experience in working in the field of IT security

**Fictitious CSIRT (step 4)**

## Defining the Business Plan

**Financial model**

Due to the fact that the company has 24x7 e-business and also a 24x7 IT department it's decided to provide full service during office hours and an on call duty for outside office hours. The services for the constituency will be provided for free, but the possibility to deliver services for external customers will be assessed during the pilot- and evaluation phase.

**Revenue model**

During the starting- and pilot-phase the CSIRT will be financed through the hosting company. During the pilot- and the evaluation phase additional funding will be discussed, including the possibility to sell services to external customers.

**Organisational model**
The hosting organisation is a small company, so the embedded model is chosen.
During office hour a staff of three people will provide the core-services (distribution of security advisories and incident handling/coordination).

The company's IT department already employs people with suitable skills. An agreement with that department is made so that the new CSIRT can request support on an ad-hoc basis when needed. Also the 2nd line of their on-call technicians can be used.
There will be a core CSIRT team with four full-time members and five additional CSIRT team members. One of those is also available on circulating shift.

**Staff**
The CSIRT team leader has a background in security and 1st and 2nd level support and has done work in the resilience crisis management work field. The other three team members are security specialists. The part-time CSIRT team members from the IT department are specialists on their part of the company's infrastructure.

## *Utilisation and equipment of the office*

The equipment and utilisation of office space and the physical security are very broad topics, therefore no exhausting description can be provided in this document. This chapter is meant to give a short overview of this topic.

More info about physical security can be found at:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

**"Hardening the building"**
Because CSIRTs usually handle very sensitive information it is a good practice to let the team take control of the physical security of the office. This will depend very much on the existing facilities and infrastructure and the existing information security policy of the hosting company.

Governments, for example, work with classification schemes and are very strict on how to handle confidential information. Check with your own company or institution about local rules and policies.

Usually a new CSIRT has to depend on the cooperation of its hosting organisation to learn about local rules, policies and other legal issues.

An exhaustive description of all equipment and security measures that will be needed is out of this document's scope. However below you will find a short list of the basic facilities for your CSIRT:

**General rules for the building**

- Use access controls
- Make the CSIRT office, at least, only accessibly to CSIRT staff.
- Monitor the offices and entrances with cameras.
- Archive confidential information in lockers or in a safe.
- Use secure IT systems.

**General rules for IT equipment**

- Use equipment that the staff can support
- Harden all systems
- Patch and update all your systems before connecting them to the internet
- Use security software (Firewalls, multiple anti-virus scanners, anti-spyware, etc.)

**Maintaining communication channels**

- Public Website
- Closed member area on the Website
- Web-forms to report incidents
- Email (PGP / GPG / S/MIME support)
- Mailing list software
- Have a dedicated telephone number available for the constituency:
    - Phone
    - Fax
    - SMS

**Record tracking system(s)**

- Contact database with details of team members, other teams, etc.
- CRM tools
- Incident handling ticket system

**Use the “corporate style” from the beginning for**

- Standard email and advisory bulletin lay-out
- ‘Old fashioned’ paper letters
- Monthly or annual reports
- Incident report form

**Other issues**

- Foresee out-of-band communication in case of attacks
- Foresee redundancy on internet connectivity

For more information about specific CSIRT tooling see the chapter *8.5 Available CSIRT Tooling.*

### *Developing an Information security policy*

Depending on the kind of CSIRT, you will have a customised information security policy. Apart from describing the desired state of operational and administrative processes and procedures, such policy has to be in line with legislation and standards, in particular with regard to the liability of the CSIRT. The CSIRT is usually bound by national laws and regulations, which are often implemented in the context of European legislation (usually Directives) and other international agreements. Standards are not necessarily binding directly, but can be mandated or recommended by laws and regulations.

Below is a short list of possible laws and policies:

**National**

- Various laws on information technology, telecommunication, media
- Laws on data protection and privacy
- Laws and regulations on data retention
- Legislation on finance, accounting, and corporate management
- Codes of conduct for corporate governance and IT governance

**European**

- Directive on electronic signatures (1993/93/EC)
- Directives on data protection (1995/46/EC) and privacy in electronic communications (2002/58/EC)
- Directives on electronic communication networks and services (2002/19/EC – 2002/22/EC)
- Directives on Company Law (e.g. 8th Company Law Directive)

**International**

- Basel II agreement (especially with regard to management of operational risk)
- Council of Europe’s Convention on Cybercrime
- Council of Europe’s Convention on Human Rights (article 8 on privacy)
- International Accounting Standards (IAS; they mandate to some extent IT controls)

**Standards**

- British Standard BS 7799 (Information Security)
- International Standards ISO2700x (Information Security Management Systems)
- German IT-Grundschutzbuch, French EBIOS and other national variations

To determine if your CSIRT is acting in accordance with national and international legislation, please consult your legal advisor.

The most basic questions to be answered in your information handling policies are:

- How is incoming information "tagged" or "classified"?
- How is information handled, especially with regard to exclusivity?
- What considerations are adopted for the disclosure of information, especially if incident-related information is passed on to other teams or sites?

- Are there legal considerations to take into account with regard to information handling?
- Do you have a policy on the use of cryptography to protect exclusivity & integrity in archives and/or data communication, especially e-mail?
- Does this policy include possible legal boundary conditions such as key escrow or enforceability of decryption in case of law suits.

**Fictitious CSIRT (step 5)**

**Office equipment and location**

Due to the fact that the hosting company already has efficient physical security in place, the new CSIRT is well covered in that aspect. A so called “war room” is provided for enabling coordination in the case of an emergency. A safe is purchased for the encryption material and sensitive documents. A separate telephone line was established including a switchboard for facilitating the hotline during office hours and the “on-call” duty mobile phone for the time outside office hours with the same phone number.

Existing equipment and the corporate website to announce CSIRT related information can also be used. A mailing-list is installed and maintained, with a restricted part for the communication among team members and with other teams. All contact details of the staff members is stored in a database, a print-out is kept in the safe.

**Regulation**

Due to the fact that the CSIRT is embedded in a company with existing information security policies the according policies for the CSIRT have been established with the help of the legal adviser of the company.

## *Search for cooperation between other CSIRTs and possible national initiatives*

The existence of other CSIRT initiatives and the strong need for cooperation between them has already been mentioned a couple of times in this document. It’s good practice to contact other CSIRTs as early as possible to get the necessary contact with the CISRT communities. Usually other CSIRTs are very open to help newly built teams to get started.

ENISAs *Inventory of CERT activities in Europe*[14] is a very good starting point for the search for other CSIRTs in the country or for national CSIRT cooperation activities.

To get support for finding a suitable source of CSIRT information contact ENISAs CSIRT experts:

CERT-Relations@enisa.europa.eu

[14] ENISAs Inventory: http://www.enisa.europa.eu/cert_inventory/

Following is an overview of CSIRT community activities. Please refer to the *Inventory* for a more comprehensive description and further information.

### European CSIRT initiative

### TF-CSIRT[15]

The TF-CSIRT Task Force promotes the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. The main goals of this Task Force is to provide a forum for exchanging experiences and knowledge, to establish pilot services for the European CSIRTs community and assist the establishment of new CSIRTs.

The main goals of the Task Force are:

- To provide a forum for exchanging experiences and knowledge
- To establish pilot services for the European CSIRTs community
- To promote common standards and procedures for responding to security incidents
- To assist the establishment of new CSIRTs and the training of CSIRTs staff.
- The activities of TF-CSIRT are focused on Europe and neighbouring countries, in compliance with the Terms of Reference approved by the TERENA Technical Committee on 15 September 2004.

### Global CSIRT initiative

### FIRST[16]

FIRST is the premier organisation and recognised global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents - reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organisations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services.

**Fictitious CSIRT (step 6)**

**Looking for cooperation**

By using ENISAs Inventory quickly some CSIRTs in the same country were found and contacted. A site visit was arranged with one of them for the newly hired team leader. He learned about national CSIRT activities and attended a meeting.
This meeting was more than helpful for collecting examples of working methods and get support by a couple of other teams.

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

# 7 Promoting the Business Plan

We have taken the following steps so far:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents
5. Defining the mission statement
6. Developing the Business Plan
    a. Defining the financial model
    b. Defining the organisational structure
    c. Starting to hire staff
    d. Utilising and equipping the office
    e. Developing an Information security policy
    f. Looking for cooperation partners

>> The next step is to put the above in a project plan and get started!

A good start for defining your project is coming up with a business case. This business case will be used as basis for the project plan and will also be used to apply for management support and gain budget or other resources.

It proved useful to continuously report to the management to keep the awareness high for IT security problems and by this for continuously support for the own CSIRT.

Starting a business case begins with analysing the problems and opportunities by using an analysis model, described in chapter *5.3 Analysis of the constituency*, and search close contact to the potential constituency.

As described earlier there are is a lot to think about when starting a CSIRT. It's best to adjust the above mentioned material to the CSIRTs needs as they develop.

Its good practice, when reporting to the management, to make the own case as up-to-date as possible by using recent articles from newspapers or the internet and explain why the CSIRT service and internal coordination of incidents are crucial for secure business assets. It's also necessary to make clear that only continuously support in matters of IT security lead to a stable business, especially for a company or an institution that is dependent on IT

(A prominent phrase by Bruce Schneier brings this to the point: *"Security is not a product but a process*[17]*!"*)

A famous tool for illustrating security problems is the following graph provided by the CERT/CC:

[17] Bruce Schneier: http://www.schneier.com/

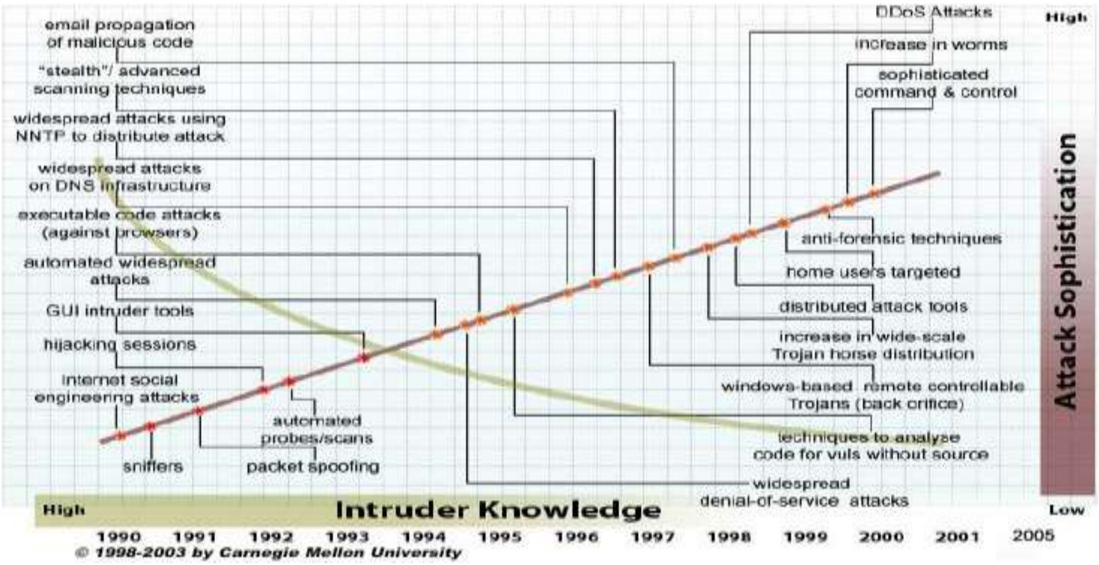


*Fig. 8 Intruder knowledge versus attack sophistication (source CERT-CC[18])*

It visualises the trends in IT security, especially the decrease in the necessary skills to carry out increasingly sophisticated attacks.

Another point to mention is the continuously shrinking time window between the availability of software updates for vulnerabilities and the starting of attacks against them:

| **Patch -> Exploit** | |
|---|---|
| Nimda: | 11 month |
| Slammer: | 6 month |
| Nachi: | 5 month |
| Blaster: | 3 weeks |
| Witty: | 1 day (!) |

| **Spreading rate** | |
|---|---|
| Code red: | Days |
| Nimda: | Hours |
| Slammer: | Minutes |

Gathered incident data, potential improvements and lessons learned make also a good presentation.

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

### *Description of business plans and management triggers*

A presentation for the management including the promotion of the CSIRT alone do not make a business case, but if carried out in an appropriate manner it will lead to support from the management for the CSIRT in most cases. The business case on the other hand should not only be seen merely as a management exercise but should also be used for the communication to the team and the constituency. The term business case might sound very commercial and far away from daily CSIRT practice, but it provides good focus and direction when setting up a CSIRT.

The answers to the following questions might be used to design a good business case (the given examples are hypothetical and used merely for illustration. The “real” answers are highly dependent on the “real” circumstances).

- What is the problem?
- What would you like to achieve with your constituents?
- What happens if you do nothing?
- What happens if you take action?
- What is it going to cost?
- What is going to gain?
- When do you start and when is it finished?

**What is the problem?**

In most cases the idea to set up a CSIRT arises when IT security has become a vital part of the core-business of a company or institution and when IT security incidents become a business risk, making security mitigation a normal business operation.

The majority of companies or institutions have a regular support department or a helpdesk but in most cases security incidents are handled insufficiently and not as structured as they should be. In most cases the security incident work field needs special skills and attention. Having a more structured approach is also beneficial and will mitigate business risks and damage to the company.

The problem in most cases is that there is a lack of coordination and that existing knowledge is not used to handle incidents, which could prevent them from happening in the future and prevent possible financial losses and / or damage to an institution’s reputation.

**What would are the goals to be achieved with the constituency?**

As explained earlier your CSIRT will serve its constituents and assist them in solving IT security incidents and problems. Raising the level of IT security knowledge and achieving a security aware culture are additional goals.

This culture endeavours proactive and preventative measures taken from the start and therefore reducing operational costs.

Introducing this culture of cooperation and assistance to a company or institution can in most cases stimulate efficiency in general.

**What happens if nothing is done?**
A non-structured way of handling IT security may lead to further damage, not least to the reputation of the institution. Financial losses and legal implications might be other results.

**What happens if action is taken?**
The awareness concerning the occurrence of security problems is raised. This helps to solve them more efficiently and prevent future losses.

**What is it going to cost?**
Depending on the organisational model it will cost the salaries of the CSIRT team members and organisation, equipment, tooling and software licences.

**What is it going to gain?**
Depending on the business and the losses in the past it will gain more transparency in procedures and security practices, therefore protecting essential business assets.

**What is the timeline?**
See chapter *12. Description of the Project plan* for the description of a sample project plan.

**Examples of existing business cases and approaches**
Here are some examples for CSIRT business cases that are worth to study:

- http://www.cert.org/csirts/AFI_case-study.html
  Creating a Financial Institution CSIRT: A Case Study

  The purpose of this document is to share lessons learned by a financial institution (referred to in this document as AFI) as they developed and implemented both a plan to address security concerns and a Computer Security Incident Response Team (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Summary of the business case of CERT POLSKA (slideshow in PDF format).

- http://www.auscert.org.au/render.html?it=2252
  Forming an Incident Response Team (IRT) in the 1990s can be a daunting task. Many people forming an IRT have no experience with doing this. This paper examines the role an IRT may play in the community, and the issues that should be addressed both during the formation and after commencement of operations. It may be of benefit to existing IRTs as it may raise awareness of issues not previously addressed.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Case Study in Information Security, Securing the Enterprise, By: Roger Benton

  This practical is a case study of Insurance Company's migration to an enterprise-wide security system. It is the intent of this practical to provide a path to follow when creating or migrating to a security system. Initially, a primitive online security system was the only mechanism to control access to corporate data. The exposures were severe - there were no integrity controls outside of the online environment. Anyone with basic programming skills could add, change and/or delete production data.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriott's e-security strategy: business-IT collaboration

  The experience of Marriott International, Inc.'s Chris Zoladz, e-business security is a process, not a project. That was the message Zoladz delivered at the recent E-Security Conference and Expo in Boston, sponsored by the Intermedia Group. As vice president of information protection for Marriott, Zoladz reports through the legal department, although he is not a lawyer. His function is to identify where Marriott's most valuable business information is stored and how it moves within and outside the company. Marriott has a separate responsibility defined for the technical infrastructure supporting security, which is given to the IT security architect.

**Fictitious CSIRT (step 7)**

**Promoting the Business Plan**

It's decided to collect facts and figures from the company's history. This is more than useful for a statistical overview of the IT security situation. This collection should be continued when the CSIRT is up and running, to keep the statistics up-to-date.

Other national CSIRTs were contacted and interviewed about their business cases. They provided support by compiling some slides with information about recent developments in IT security incidents and about costs of incidents.

In this example case of Fictious CSIRT there was no pressing need to convince the management about the importance of IT business, and so it was not hard to get the go-ahead for the first step. A business case and a project plan where prepared, including an estimation of the set-up costs and the cost of operation.

# 8 Examples of operational and technical procedures (workflows)

We have taken the following steps so far:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents.
5. Defining the mission statement.
6. Developing the Business Plan.
   a. Defining the financial model.
   b. Defining the organisational structure.
   c. Starting to hire staff.
   d. Utilising and equipping the office.
   e. Developing an Information security policy
   f. Looking for cooperation partners.
7. Promoting the Business Plan.
   a. Have the business case approved.
   b. Fit everything into a project plan.

>> The next step is: making the CSIRT operational

Having well defined workflows in place will improve the quality and the needed time per incident or vulnerability case.

As described in the example boxes, Fictitious CSIRT will offer the basic CSIRT core-services:

- Alerts and Warnings
- Incident Handling
- Announcements

This chapter provides examples of workflows that describe the core-services of a CSIRT. This chapter also contains information about collecting information from different sources, checking it on relevance and authenticity and redistributing it to the constituency. And finally this chapter contains examples of the most basic procedures and specific CSIRT tooling.

### Assess the installation base of the constituency

The first step is to gather an overview of the IT systems installed at your constituency. By this the CSIRT can evaluate the relevance of incoming information and filter it before redistribution, so the constituents will not get overwhelmed with information that is basically useless for them.

Its good practice to begin simple, for example by using an excel sheet like the following:

| Category | Application | Software product | Version | OS | OS version | Constituent |
|---|---|---|---|---|---|---|
| Desktop | Office | Excel | x-x-x | Microsoft | XP-prof | A |
| Desktop | Browser | IE | x-x- | Microsoft | XP-prof | A |
| Network | Router | CISCO | x-x-x | CISCO | x-x-x- | B |
| Server | Server | Linux | x-x-x | L-distro | x-x-x | B |
| Services | Web server | Apache | | Unix | x-x-x | B |

With the filter function in excel it’s very easy to select the proper software and see which constituent is using which kind of software.

### *Generating Alerts, Warnings and Announcements*

The generation of alerts, warnings and announcements all follow the same workflows:

- The collection of information
- Evaluation of the information on relevance and source
- Risk assessment based on the gathered information
- Distribution of the information

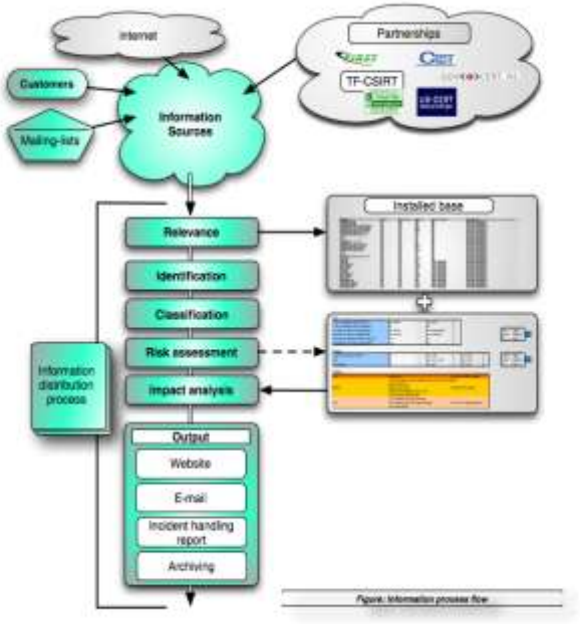


*Fig. 9 : Information process flow*

In the following paragraphs this workflow will be described in more detail.

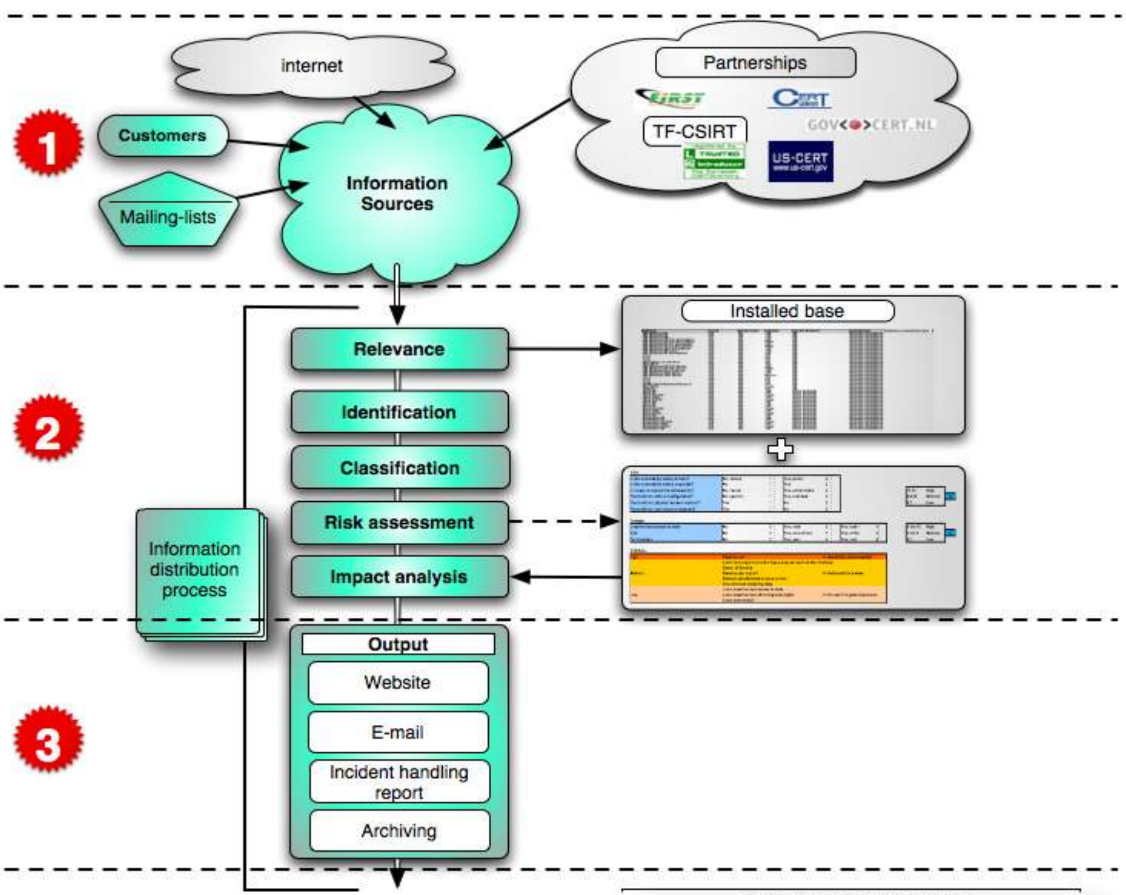


*Figure: Information process flow*

## Step 1: Collecting vulnerability information.

Usually there exist two main types of information sources that contribute information as input for the services:

- Vulnerability information about (your) IT systems
- Incident reports

Depending of the kind of business and IT infrastructure there are many public and closed sources for vulnerability information:

- Public and closed mailing lists
- Vendor vulnerability product information
- Websites
- Information on the Internet (Google, etc…)
- Public and private partnerships that provide vulnerability information (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

All this information contributes to the level of knowledge about specific vulnerabilities in IT systems.

As stated before there are a lot of good and easy accessible security information sources available in the internet. The ENISA ad-hoc working-group “CERT services” for 2006 produces at the time of writing a more comprehensive list that is supposed to be at the end of 2006[19].

## Step 2: Evaluation of the information and assessment of the risk

This step will result in an analysis of the impact of a specific vulnerability to the IT infrastructure of the constituency.

### Identification

Incoming vulnerability information always has to be identified by its source and it has to be determined whether the source is trustworthy before any information is given to the constituency. Otherwise people might get falsely alerted, what could lead to unnecessary disturbances in business processes and in the end to damage of the CSIRTs reputation.

[19] Ad-hoc WG CERT services: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

The following procedure shows an example of identifying the authenticity of a message:

***Procedure on how to identify the authenticity of a message and its source***

**General Checklist**

1. Is the source known and registered as such?
2. Does the information come via a regular channel?
3. Is there “strange” information contained that “feels” wrong?
4. Follow your feeling, there’s doubt about an information don’t act but verify again!

**E-Mail - Sources**

1. Is the source address known to the organisation and known to the source list?
2. Is the PGP-signature correct?
3. When in doubt check the full headers of a message.
4. When in doubt use “nslookup” or ”dig” to verify the senders domain[20].

**WWW - Sources**

1. Check browser certificates when connecting to a secured website (https ://).
2. Check source on content and validity (technical).
3. When in doubt, don’t click any links or download any software.
4. When in doubt have a “lookup” and “dig” done on the domain and do a “traceroute”.

**Telephone**

1. Listen carefully to the name.
2. Do you recognise the voice?
3. When in doubt ask for a telephone number and request to call back the caller.

*Fig. 10 Example of a information identification procedure*

### Relevance

The overview of installed hard- and software produced earlier can be used to filter the incoming vulnerability information on relevance, with the goal to find an answer to the questions: ”Does the constituency use this piece of software?”; “Is the information relevant for them?”

### Classification

Some information received may be classified or tagged as restricted (for example incoming incident reports from other teams). All information has to be handled according to the demand of the sender and according to the own information security policy. A good basic rule is “*Don’t distribute information if it’s not clear that it is meant to be; when in doubt ask the sender for permission to do so.*”

[20] Tools for checking identities in the CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

**Risk assessment & impact analysis**

There are several methods for determining the risk and impact of a (potential) vulnerability.

Risk is defined as the potential chance that the vulnerability can be exploited. There are several important factors (among others):

- Is the vulnerability well known?
- Is the vulnerability wide spread?
- Is it easy to exploit the vulnerability?
- Is it a remotely exploitable vulnerability?

All these questions give a good sense of the seriousness of the vulnerability.
A very simple approach to calculate the risk is the following formula:

Impact = Risk X potential Damage

Potential damage could be

- Unauthorised access to data
- Denial of Service (DOS)
- Gaining or extending of permissions

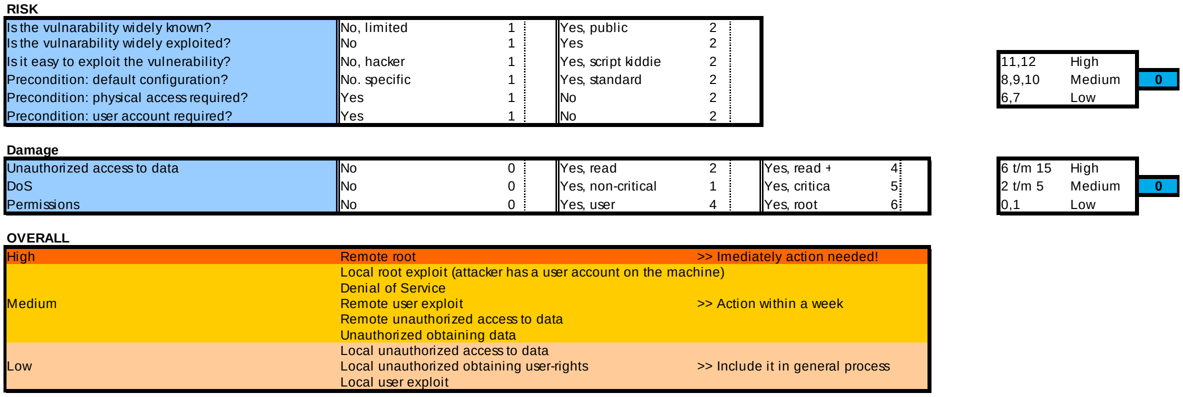
(For more elaborated classification schemes please see the end of this chapter).

With these questions answered an overall rating can be added to the advisory, informing about potential risk and damage. Often simple terms like LOW, MEDIUM and HIGH are used.

Other, more comprehensive risk assessment schemes are:

## GOVCERT.NL rating scheme[21]

The Dutch governmental CSIRT GOVCERT.NL has developed a matrix for the risk assessment that was developed at the start phase of Govcert.nl and is still updated to the latest trends.



RISK

| | | | | |
|---|---|---|---|---|
| Is the vulnarability widely known? | No, limited | 1 | Yes, public | 2 |
| Is the vulnarability widely exploited? | No | 1 | Yes | 2 |
| Is it easy to exploit the vulnerability? | No, hacker | 1 | Yes, script kiddie | 2 |
| Precondition: default configuration? | No. specific | 1 | Yes, standard | 2 |
| Precondition: physical access required? | Yes | 1 | No | 2 |
| Precondition: user account required? | Yes | 1 | No | 2 |

| | | |
|---|---|---|
| 11,12 | High | |
| 8,9,10 | Medium | 0 |
| 6,7 | Low | |

Damage

| | | | | | | |
|---|---|---|---|---|---|---|
| Unauthorized access to data | No | 0 | Yes, read | 2 | Yes, read + | 4 |
| DoS | No | 0 | Yes, non-critical | 1 | Yes, critica | 5 |
| Permissions | No | 0 | Yes, user | 4 | Yes, root | 6 |

| | | |
|---|---|---|
| 6 t/m 15 | High | |
| 2 t/m 5 | Medium | 0 |
| 0,1 | Low | |

OVERALL

| | | |
|---|---|---|
| High | Remote root | >> Imediately action needed! |
| Medium | Local root exploit (attacker has a user account on the machine)<br>Denial of Service<br>Remote user exploit<br>Remote unauthorized access to data<br>Unauthorized obtaining data | >> Action within a week |
| Low | Local unauthorized access to data<br>Local unauthorized obtaining user-rights<br>Local user exploit | >> Include it in general process |

*Fig. 11 The GOVCERT.NL rating scheme*

## EISPP Common Advisory Format Description[22]

The European Information Security Promotion Programme (EISPP) is a project co-funded by the European Community under the Fifth Framework Programme. The EISPP project aims to develop a European framework, not only to share security knowledge but also to define the content and ways of disseminating security information to SMEs. By providing European SMEs with the necessary IT security services they will be encouraged to develop their trust and usage of e-commerce leading to increased and better opportunities for new business. The EISPP is a pioneer in the European Commission's vision of forming a European network of expertise within the European Union.

## DAF Deutsches Advisory Format[23]

DAF is an initiative of the German CERT-Verbund and is a core component of an infrastructure for the generation and exchange of security advisories by different teams. DAF is especially tailored for the needs of the German CERTs; the standard is developed and maintained by CERT-Bund, DFN-CERT, PRESECURE and Siemens-CERT.

[21] Vulnerability matrix: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

## Step 3: Distribution of the information

A CSIRT can choose from several distribution methods depending on the wishes of the constituents and your communication strategy.

- Website
- Email
- Reports
- Archiving and research

Security advisories distributed by a CSIRT should always follow the same structure. This will enhance the readability and the reader will quickly find all the relevant information.

An advisory should at least contain the following information:

**Title of the advisory**
……………………………………………………………………………………

**Reference number**
……………………………
**Systems affected**
**-** ……………………………
**-** ……………………………

**Related OS + version**
……………………………
**Risk** (High-Medium-Low)
………
**Impact/potential damage** (High-Medium-Low)
………
**External id's:** (CVE, Vulnerability bulletin ID's)
…………

**Overview of vulnerability**
……………………………………………………………

**Impact**
……………………………………………………………

**Solution**
……………………………………………………………

**Description (details)**
……………………………………………………………

**Appendix**
……………………………………………………………

*Fig. 12 Sample advisory scheme*

See chapter *10. Exercise* for a complete example of a security advisory.

## Doing Incident Handling

As mentioned in the introduction of this chapter, the process of information handling during incident handling is very similar to that used during the compilation of alerts, warnings and announcements. But the information gathering part usually is different, as the normal way to get incident related data is either by receiving incident reports from the constituency or other teams, or by receiving feedback from involved parties during the incident handling process. Information usually flows by (encrypted) e-mail; sometimes the use of telephone or fax is necessary.

When receiving information via telephone, it's good practice to note down every single detail at once either by using an incident handling/reporting tool or by making a memo. It is necessary to immediately (before the call ends) generate an incident number (if none exists for this incident so far) and to issue it to the reporter on the phone (or by a summarising e-mail sent afterwards) as a reference for further communication.

The rest of this chapter describes the basic process of incident handling. A very in-depth analysis of the complete process of incident management and all involved workflows and sub-workflows can be found in the CERT/CC documentation *Defining Incident Management processes for CSIRTs*[24].

[24] Defining Incident Management Processes: http://www.cert.org/archive/pdf/04tr015.pdf

Basically, incident handling follows the following workflow:

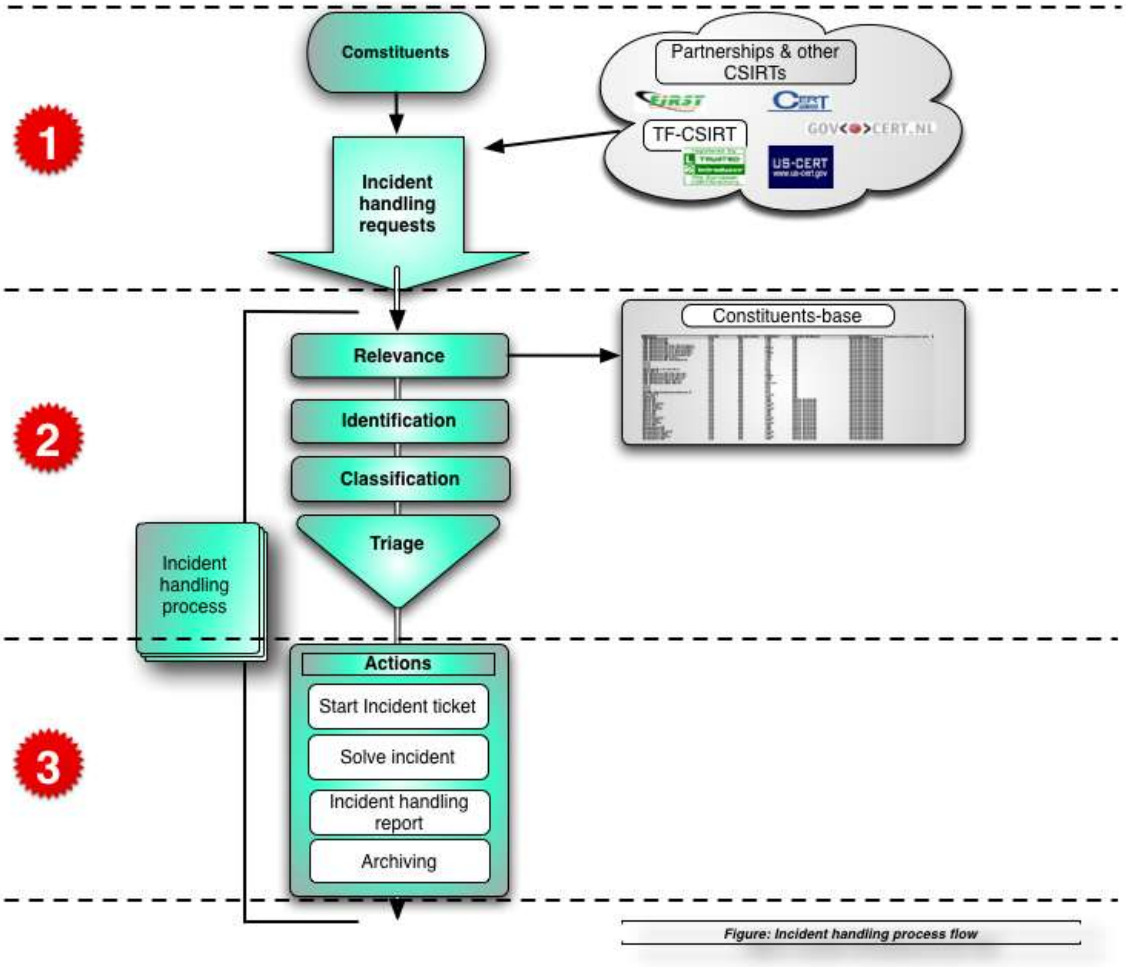


*Fig. 13 Incident process flow*

## Step 1: Receiving incident reports

As mentioned before, incident reports reach a CSIRT via several channels, mostly e-mail but also telephone or fax.

As mentioned before, it is good practice to note down all the details in a fixed format while receiving an incident report. By this it is ensured that no crucial information is left out. Following a sample scheme can be found:

### INCIDENT REPORTING FORM

*Please fill out this form and Fax or email it to: …………….*
*Lines marked with * are required.*

*Name and Organisation*

1. Name*:
2. Name of Organisation*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

*Affected Host(s)*

9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Security:
18. Hostname & IP:
19. Protocol/port:

*Incident*

20. Reference number ref #:
21. Type of Incident:
22. Incident Started:
23. This is an ongoing incident: YES NO
24. Time and Method of Discovery:
25. Known Vulnerabilities:
26. Suspicious Files:
27. Countermeasures:
28. Detailed description*:

*Fig. 14 Contents of an incident report*

## 2 Step 2: Incident evaluation

During this step the authenticity and the relevance of a reported incident is checked and the incident is classified.

### Identification

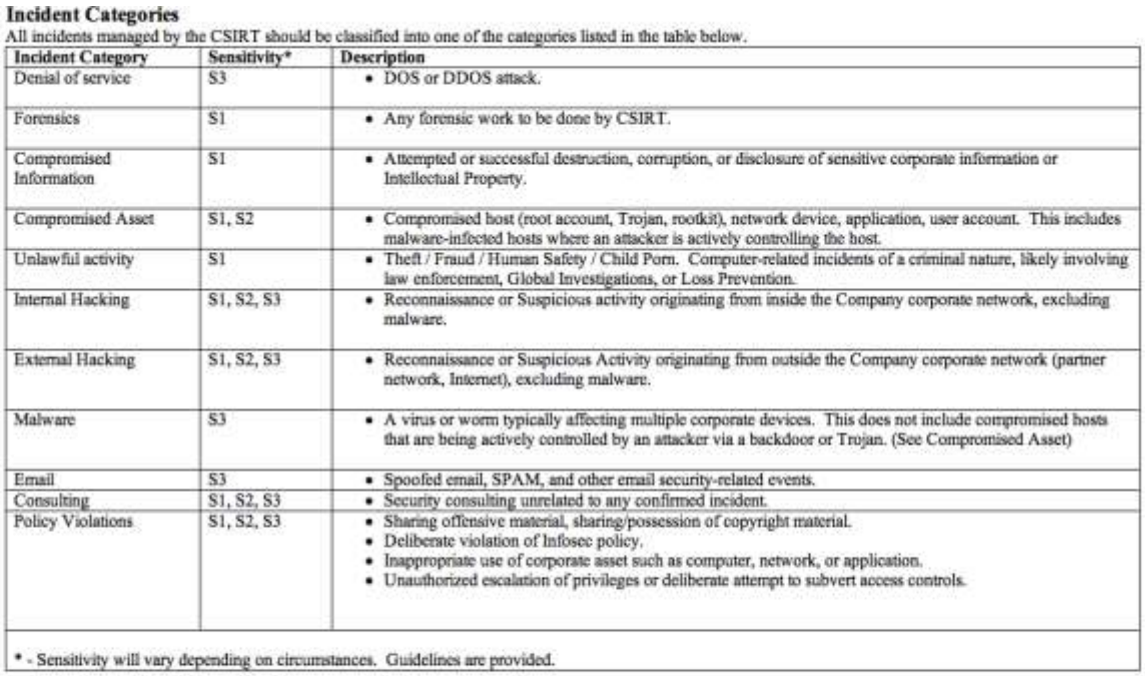
To prevent any unnecessary action it's a good habit to check if the originator is trustworthy and if the originator is one of your, or a colleague CSIRTs constituents. Similar rules as described in chapter *8.2 Generating Alerts* apply.

### Relevance

With this step you check if the incident-handling request originates from the CSIRTs constituency, or if the reported incident involves IT systems form the constituency. If neither of the above applies, the report is usually re-routed to the right CISRT[25].

### Classification

With this step the triage is prepared by classifying the severity of the incident. It's outside the scope of this document to go into details of incident classification. A good start is to utilise the CSIRT Case Classification scheme (Example for Enterprise CSIRT):



**Incident Categories**

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

| Incident Category | Sensitivity* | Description |
|---|---|---|
| Denial of service | S3 | • DOS or DDOS attack. |
| Forensics | S1 | • Any forensic work to be done by CSIRT. |
| Compromised Information | S1 | • Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property. |
| Compromised Asset | S1, S2 | • Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host. |
| Unlawful activity | S1 | • Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention. |
| Internal Hacking | S1, S2, S3 | • Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware. |
| External Hacking | S1, S2, S3 | • Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware. |
| Malware | S3 | • A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset) |
| Email | S3 | • Spoofed email, SPAM, and other email security-related events. |
| Consulting | S1, S2, S3 | • Security consulting unrelated to any confirmed incident. |
| Policy Violations | S1, S2, S3 | • Sharing offensive material, sharing/possession of copyright material.<br>• Deliberate violation of Infosec policy.<br>• Inappropriate use of corporate asset such as computer, network, or application.<br>• Unauthorized escalation of privileges or deliberate attempt to subvert access controls. |

* - Sensitivity will vary depending on circumstances. Guidelines are provided.

*Fig. 15 Incident classification scheme (source: FIRST)*[26]

[25] Tools for checking identities in the CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] CSIRT Case Classification http://www.first.org/resources/guides/csirt_case_classification.html

**Triage**

Triage is a system used by medical or emergency personnel to ration limited medical resources when the number of injured needing care exceeds the resources available to perform care so as to treat the greatest number of patients possible[27].

The CERT/CC gives the following description:

*Triage is an essential element of any incident management capability, particularly for any established CSIRT. Triage is on the critical path for understanding what is being reported throughout the organisation. It serves as the vehicle by which all information flows into a single point of contact, allowing for an enterprise view of ongoing activity and a comprehensive correlation of all reported data. Triage allows for an initial assessment of an incoming report and queues it for further handling. It also provides a venue for beginning the initial documentation and data entry of a report or request, if this has not already been done in the Detect process.*

*The triage function provides an immediate snapshot of the current status of all activity reported— what reports are open or closed, what actions are pending, and how many of each type of report has been received. This process can help to identify potential security problems and prioritise the workload. Information gathered during triage can also be used to generate vulnerability and incident trends and statistics for upper management*[28]*.*

Triage should only been done by the most experienced team members, because it requires deep understanding of the potential impacts of incidents on specific parts of the constituency and the ability to decide who would be the appropriate team member to handle that incident.

[27] Triage in Wikipedia: http://en.wikipedia.org/wiki/Triage

[28] Defining Incident Management Processes: http://www.cert.org/archive/pdf/04tr015.pdf

## Step 3: Actions

Usually triaged incidents go into a request queue in an incident handling tool that is used by one or more incident handlers, who basically follow these steps.

### Start incident ticket

The incident ticket number might already have been generated in a previous step (for example when the incident was reported via telephone). If not, the first step is to create such a number that will be used in all further communication about this incident.

### Incident lifecycle

Handling an incident does not follow a line of steps that finally lead to a solution, but it rather follows a circle of steps that are repeatedly applied until the incident is finally solved and all involved parties have all necessary information. This circle, also often referred to as the "Incident Lifecycle", contains the following processes:

*Analysis:* All details of the reported incident are analysed.

*Obtain contact information*: To be able to further report information related to the incident to all involved parties, like other CSIRTs, victims and probably the owners of systems that might have been misused for an attack.

*Provide technical assistance*: Help victims to quickly recover from the results of the incident and collect more information about the attack.

*Coordination:* Inform other involved parties like the CSIRT responsible for the IT system used for an attack, or other victims.

This structure is called a "lifecycle", because one of the steps leads to another and the last one, the coordination-part, then might again lead to a new analysis, and the cycle starts again. The process ends when all involved parties received and reported all necessary information.

Please refer to the CERT/CC CSIRT handbook for a more detailed description of the incident lifecycle[29].

### Incident handling report

Be prepared for questions from management about incidents by compiling a report. It's also good practice to write a document (for internal use only) about "lessons learned" to teach the staff and to avoid mistakes in future incident handling processes.

### Archiving

Look into the archiving rules described earlier in chapter *6.6 Developing an Information security policy*.

Please refer to the Annex section *A.1 Further reading* for comprehensive guides on incident management and the incident lifecycle.

[29] CSIRT handbook: http://www.cert.org/archive/pdf/csirt-handbook.pdf

### *Example of a response timetable*

The definition of response times is often neglected but must be part of every well constructed service level agreement (SLA) between a CSIRT and its constituency. Giving timely feedback to constituents during incident handling is crucial, both for the constituents' own liabilities and for the reputation of the team.
The response times must be clearly communicated to the constituency to avoid wrong expectations. The following very basic timetable can be used as a starting point for a more detailed SLA with a CSIRTs constituency.

Here is an example of a practical response timetable from the point of an incoming request for assistance:

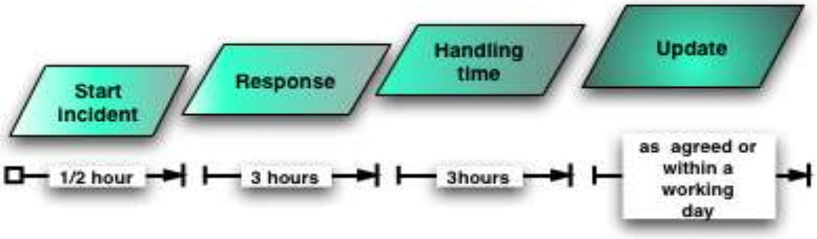


*Fig. 16 Example response timetable*

It's also good practice to instruct the constituency about their own response times, especially when to contact the CSIRT in case of an emergency. In most cases it's better to contact their CSIRT at an early stage, and it's good practice to encourage the constituency to do so when in doubt.

## Available CSIRT tooling

This chapter provides some pointers to common tools used by CSIRTs. It only provides examples, more pointers can be found in the *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

### Email and message encryption software

- GNUPG http://www.gnupg.org/
  GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC2440. GnuPG allows you to encrypt and sign your data and communication.

- PGP http://www.pgp.com/
  Commercial variant

### Incident handling tool

Administrate incidents and their follow up, keeping track of actions.

- RTIR http://www.bestpractical.com/rtir/
  RTIR is a free open source incident handling system designed with the needs of CERT teams and other incident-response teams in mind.

### CRM tools

When you have a lot of different constituents and need to track down all appointments and details, a CRM database is helpful. There are many different variations, here are some examples:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (Free open source version) http://www.sugarforge.org/

### Information checking

- Website watcher http://www.aignes.com/index.htm
  This program monitors websites for updates and changes.

- Watch that page http://www.watchthatpage.com/
  The service sends information about changes in websites by e-mail (free and commercial).

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

### Finding contact information

Finding the correct contact to report incidents to is not a simple task. There are a couple of information sources that can be used:

- RIPE[31]
- IRT-object[32]
- TI[33]

Additionally, the CHIHT lists some tools for finding contact information[34].

**Fictitious CSIRT (step 8)**

**Establishing process flows and operational and technical procedures**

Fictious CSIRT focuses on delivering core CSIRT services:

- Alerts and Warnings
- Announcements
- Incident Handling

The team developed procedures that work well and that are easily understandable by every team member. Fictious CSIRT also hired a legal expert to deal with liabilities and the information security policy. The team adopted some useful tools and found helpful information about operational issues by discussing with other CSIRTs.

A fixed template for security advisories and incident reports was generated. The team uses RTIR for incident handling.

[31] RIPE whois: http://www.ripe.net/whois

[32] IRT-object in the RIPE database: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Tools for checking identities in the CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

# 9 CSIRT training

We have taken the following steps so far:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents.
5. Defining the mission statement.
6. Developing the Business Plan.
   a. Defining the financial model.
   b. Defining the organisational structure.
   c. Starting to hire staff.
   d. Utilising and equipping the office.
   e. Developing an Information security policy
   f. Looking for cooperation partners.
7. Promoting the Business Plan.
   a. Have the business case approved.
   b. Fit everything into a project plan.
8. Making the CSIRT operational.
   a. Creating workflows
   b. Implementing CSIRT tooling

>> The next step is: training the staff

This chapter lists the two main sources for dedicated CSIRT training: TRANSITS and the CERT/CC courses.

## *TRANSITS*

TRANSITS has been a European project to promote the establishment of Computer Security Incident Response Teams (CSIRTs) and the enhancement of existing CSIRTs by addressing the problem of the shortage of skilled CSIRT staff. This goal has been addressed by providing specialist training courses to train staff of (new) CSIRTs in the organisational, operational, technical, market and legal issues involved in providing CSIRT services.

In particular, TRANSITS has

- developed, updated and regularly revised modular training course material
- organized training workshops where the course materials were delivered
- enabled the participation of staff members of (new) CSIRTs in these training workshops, with a particular emphasis on the participation from the EU Accession States
- disseminated the training course materials and ensured exploitation of the results[35].

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

ENISA is facilitating and supporting the TRANSITS courses. If you want to know how to apply for courses, the requirements and costs, please contact ENISAs CSIRT experts:

CERT-Relations@enisa.europa.eu

Please find sample course material in the annex of this document!

### CERT/CC

The complexity of computer and network infrastructures and the challenge of administration make it difficult to properly manage network security. Network and system administrators do not have sufficient people and security practices in place to defend against attacks and minimise damage. As a result there are a rising number of computer security incidents.
When computer security incidents occur, organisations must respond quickly and effectively. The faster an organisation recognises, analyses, and responds to an incident, the better it can limit damage and lessen recovery costs. Establishing a computer security incident response team (CSIRT) is a great way to provide this rapid response capability as well as help prevent future incidents.

CERT-CC offers courses for managers and technical personnel in areas such as creating and managing computer security incident response teams (CSIRTs), responding to and analysing security incidents, and improving network security. Unless otherwise noted, all courses are held in Pittsburgh, PA. Members of our staff also teach courses in security at Carnegie Mellon University.

Available CERT/CC Courses[36] dedicated to CSIRTs

Creating a Computer Security Incident Response Team (CSIRT)
Managing Computer Security Incident Response Teams (CSIRTs)
Fundamentals of Incident Handling
Advanced Incident Handling for Technical Staff

Please find sample course material in the annex of this document!

**Fictitious CSIRT (step 9)**

**Training the staff**

Fictious CSIRT decides to send all their technical staff to the next available TRANSITS courses. The team leader additionally attends the *Managing a CSIRT* course from CERT/CC.

[36] CERT/CC courses: http://www.sei.cmu.edu/products/courses

# 10 Exercise: producing an advisory

We have taken the following steps so far:

1. Understanding what a CSIRT is and what benefits it might provide.
2. To what sector will the new team deliver its services to?
3. What kinds of services a CSIRT can provide to its constituency.
4. Analysis of the environment and constituents.
5. Defining the mission statement.
6. Developing the Business Plan.
   a. Defining the financial model.
   b. Defining the organisational structure.
   c. Starting to hire staff.
   d. Utilising and equipping the office.
   e. Developing an Information security policy
   f. Looking for cooperation partners.
7. Promoting the Business Plan.
   a. Have the business case approved.
   b. Fit everything into a project plan.
8. Making the CSIRT operational.
   a. Creating workflows
   b. Implementing CSIRT tooling
9. Training your staff

>> The next step is to exercise and be ready for the real work!

For illustration this chapter describes a sample exercise for an everyday CSIRT task: creating a security advisory.

The trigger was the following original security advisory sent out by Microsoft:

| **Bulletin Identifier** | **Microsoft Security Bulletin MS06-042** |
|---|---|
| **Bulletin Title** | **Cumulative Security Update for Internet Explorer (918899)** |
| **Executive Summary** | This update resolves several vulnerabilities in Internet Explorer that could allow remote code execution. |
| **Maximum Severity Rating** | Critical |
| **Impact of Vulnerability** | Remote Code Execution |
| **Affected Software** | **Windows, Internet Explorer.** For more information, see the Affected Software and Download Locations section. |

This vendor-bulletin addresses a recently found vulnerability in Internet Explorer. The vendor publishes multiple fixes for this software for multiple versions of Microsoft Windows.

Fictious CSIRT, after receiving this vulnerability information via a mailing-list, begins with the workflow described in chapter *8.2 Generating Alerts, Warnings and Announcements*.

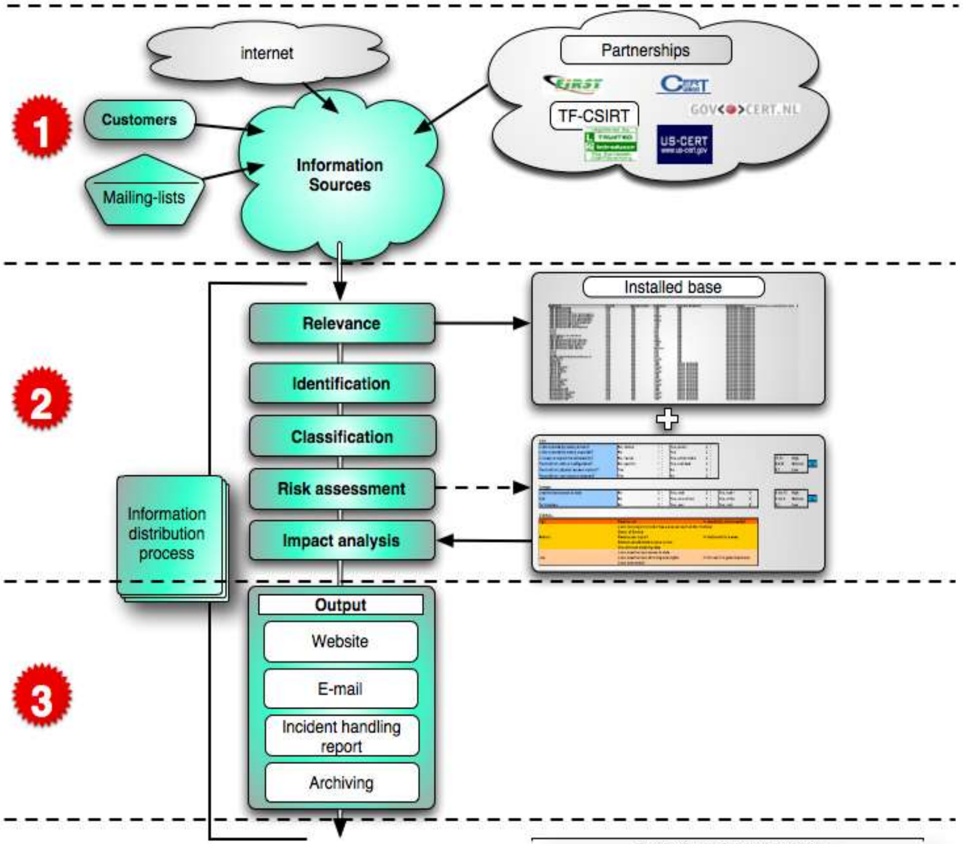


*Figure: Information process flow*

## Step 1: Collecting vulnerability information.

The first step is browsing to the website of the vendor. There Fictious CSIRT verifies the authenticity of the information and gathers further details about the vulnerability and the affected IT systems.

## 2 Step 2: Evaluation of the information and assessment of the risk

**Identification**
The information has already been verified by cross-checking the vulnerability information received by e-mail with the text on the website of the vendor.

**Relevance**
Fictious CSIRT checks the list of affected systems found on the website with the list of used systems in the constituency. It finds that at least one of their constituents uses the Internet Explorer, so the vulnerability information is indeed relevant.

| Category | Application | Software product | Version | OS | OS Version | Constituent |
|---|---|---|---|---|---|---|
| Desktop | Browser | IE | x-x- | Microsoft | XP-prof | A |

**Classification**
The information is public so it can be used and redistributed.

**Risk assessment & impact analysis**
Answering the questions shows that the risk and impact is *high* (rated *critical* by Microsoft).

**RISK**

| | |
|---|---|
| Is the vulnerability well known? | Y |
| Is the vulnerability widespread? | Y |
| Is it easy to exploit the vulnerability? | Y |
| Is it a remotely exploitable vulnerability? | Y |

**DAMAGE**
Possible impacts are remote accessibility and potentially remote code execution. This vulnerability contains multiple issues, which make the damage risk *high*.

## Step 3: Distribution

The Fictitious CSIRT is an internal CSIRT. It has email, phone and the internal website available as communication channels. The CSIRT produces this advisory, derived from the template from chapter *8.2 Generating Alerts, Warnings and Announcements*.

**Title of advisory**
Multiple vulnerabilities found in Internet explorer

**Reference number**
082006-1
**Systems affected**

- All desktop systems that run Microsoft

**Related OS + version**

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

**Risk** (High-Medium-Low)
HIGH
**Impact/potential damage** (High-Medium-Low)
HIGH
**External id's:** (CVE, Vulnerability bulletin ID's)
MS-06-42

**Overview of vulnerability**
Microsoft has found several critical vulnerabilities in Internet Explorer which can lead too remote code execution.

**Impact**
An attacker could take complete control over the system, installing programs, adding users and vie, change or delete data. Mitigating factor is that the above only can take place if the user is logged in with administrator rights. Users logged on with fewer rights could be less impacted.

**Solution**
Patch your IE immediately

**Description (details)**
See for more information ms06-042.mspx

**Appendix**
See for more information ms06-042.mspx

This output is now ready for distribution. Because it is a critical bulletin it’s advisable to also call the constituents when possible.

**Fictitious CSIRT (step 10)**

**Exercising**

During the first weeks of operations fictious CSIRT used several fictious cases (that they got as examples from other CSIRTs) that where used as exercise. Furthermore they issued a couple of security advisories based on real vulnerability information distributed by hard- and software vendors, that they fine-tuned and adjusted to the needs of the constituency.

# 11 Conclusion

Here the guide ends. The document at hand is intended for giving a very concise overview of the various processes necessary for setting up a CSIRT. It does not claim to be complete neither does it go too much into specific details. Please refer to the section *A.1 Further reading* in the annex for literature on that topic worth reading.

The next important steps for Fictious CSIRT now would be:

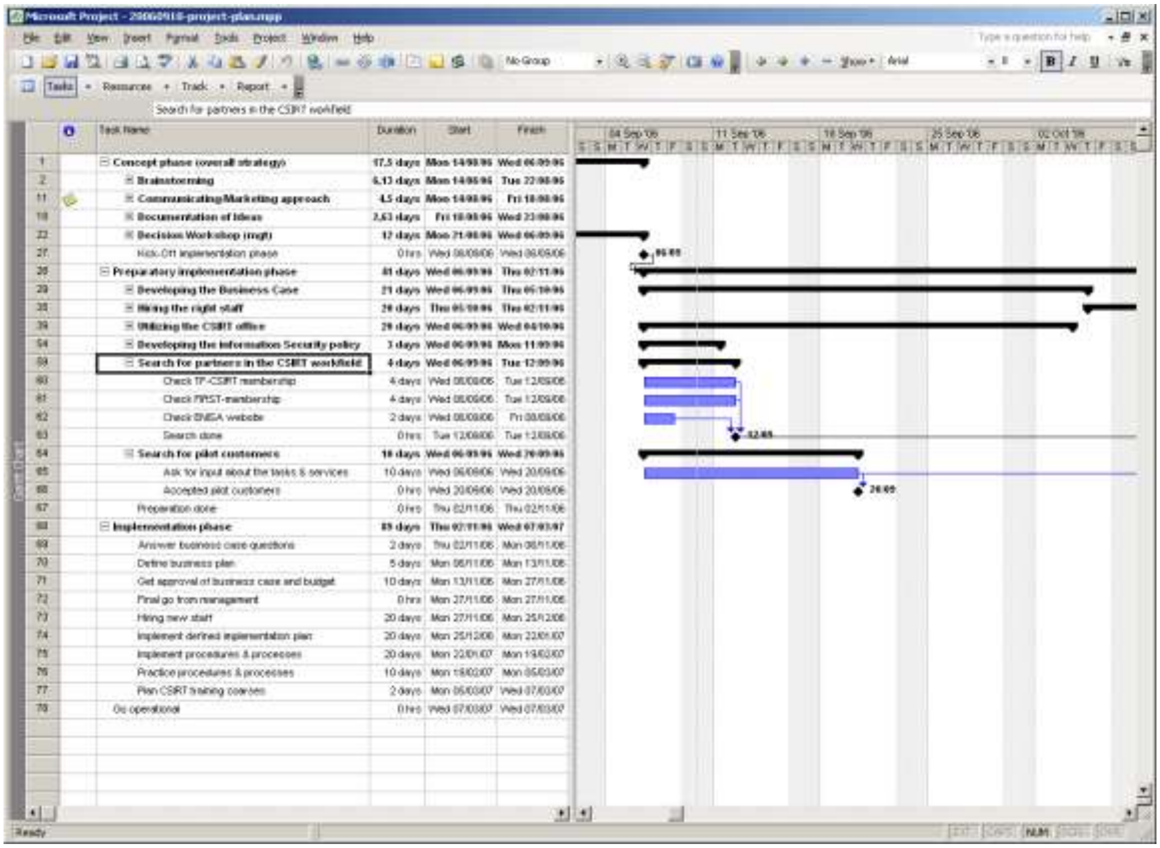
- Receive feedback from the constituency to fine-tune the provided services
- Get routine in the daily work
- Exercise emergency situations
- Stay in close touch with the various CSIRT communities with the goal to contribute to their voluntary work one day

# 12 Description of the Project Plan

*NOTE: The project plan is a first estimation on the needed time. Depending on available resources the real duration of the project might be different.*

The project plan is available in different formats on CD and the ENISA website. It completely covers all processes described in this document.

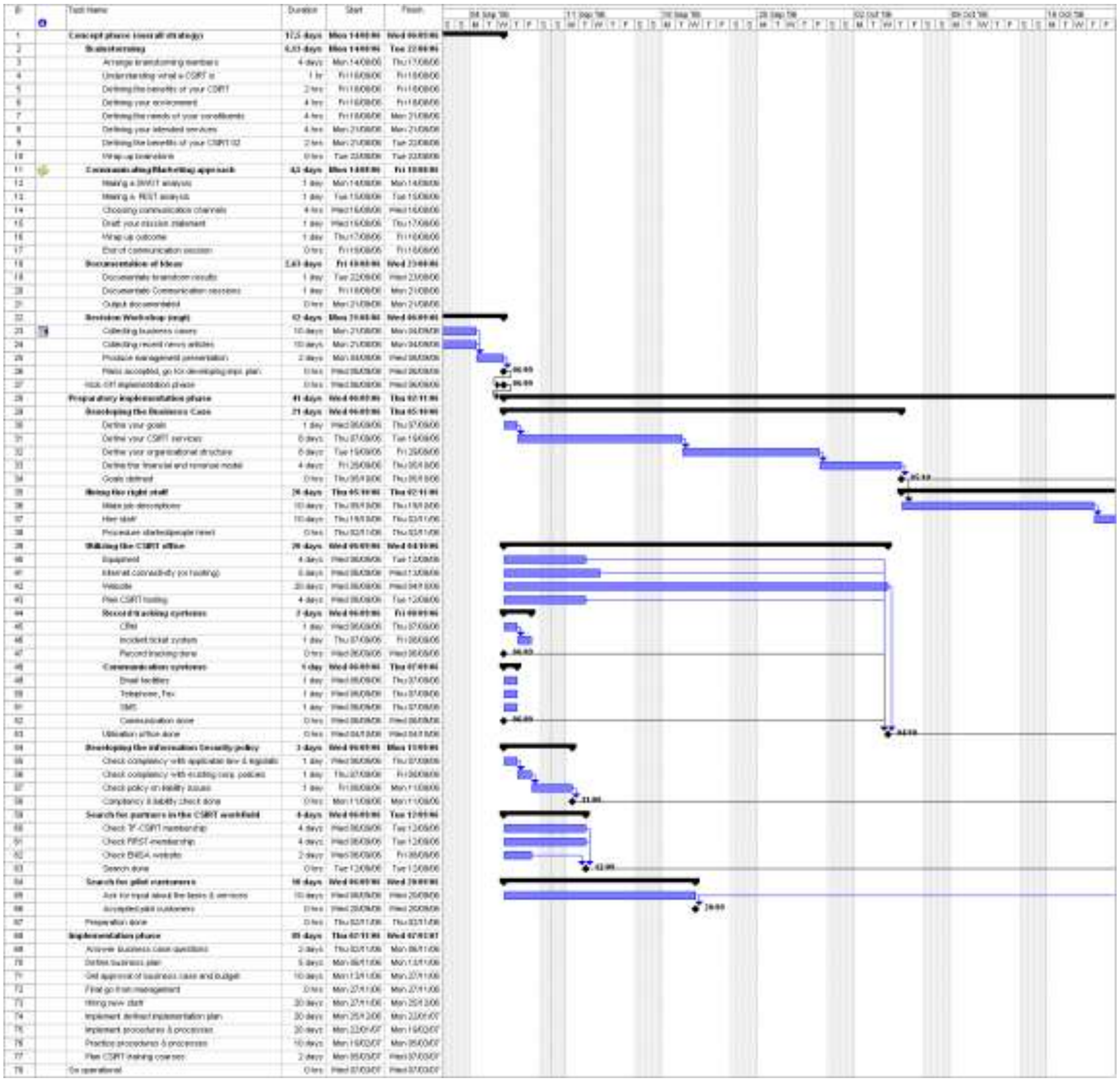
The main format will be Microsoft Project, so it can directly be used in this project management tool.


Microsoft Project - 20060918-project-plan.mpp
File Edit View Insert Format Tools Project Window Help
Type a question for help
No Group
Show
Arial
8
Tasks Resources Track Report
04 Sep '06
11 Sep '06
18 Sep '06
25 Sep '06
02 Oct '06
S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S
06/09
12/09
20/09
Gantt Chart
Ready
EXT CAPS NUM SCRL OVR

Search for partners in the CSIRT workfield

| | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 1 | Concept phase (overall strategy) | 17.5 days | Mon 14/08/06 | Wed 06/09/06 |
| 2 | Brainstorming | 6.13 days | Mon 14/08/06 | Tue 22/08/06 |
| 11 | Communicating/Marketing approach | 4.5 days | Mon 14/08/06 | Fri 18/08/06 |
| 18 | Documentation of Ideas | 2.63 days | Fri 18/08/06 | Wed 23/08/06 |
| 22 | Decision Workshop (mgt) | 12 days | Mon 21/08/06 | Wed 06/09/06 |
| 27 | Kick-Off implementation phase | 0 hrs | Wed 06/09/06 | Wed 06/09/06 |
| 28 | Preparatory implementation phase | 41 days | Wed 06/09/06 | Thu 02/11/06 |
| 29 | Developing the Business Case | 21 days | Wed 06/09/06 | Thu 05/10/06 |
| 38 | Hiring the right staff | 21 days | Thu 05/10/06 | Thu 02/11/06 |
| 39 | Utilizing the CSIRT office | 21 days | Wed 06/09/06 | Wed 04/10/06 |
| 54 | Developing the information Security policy | 3 days | Wed 06/09/06 | Mon 11/09/06 |
| 59 | Search for partners in the CSIRT workfield | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 60 | Check TF-CSIRT membership | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 61 | Check FIRST-membership | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 62 | Check ENISA website | 2 days | Wed 06/09/06 | Fri 08/09/06 |
| 63 | Search done | 0 hrs | Tue 12/09/06 | Tue 12/09/06 |
| 64 | Search for pilot customers | 10 days | Wed 06/09/06 | Wed 20/09/06 |
| 65 | Ask for input about the tasks & services | 10 days | Wed 06/09/06 | Wed 20/09/06 |
| 66 | Accepted pilot customers | 0 hrs | Wed 20/09/06 | Wed 20/09/06 |
| 67 | Preparation done | 0 hrs | Thu 02/11/06 | Thu 02/11/06 |
| 68 | Implementation phase | 89 days | Thu 02/11/06 | Wed 07/03/07 |
| 69 | Answer business case questions | 2 days | Thu 02/11/06 | Mon 06/11/06 |
| 70 | Define business plan | 5 days | Mon 06/11/06 | Mon 13/11/06 |
| 71 | Get approval of business case and budget | 10 days | Mon 13/11/06 | Mon 27/11/06 |
| 72 | Final go from management | 0 hrs | Mon 27/11/06 | Mon 27/11/06 |
| 73 | Hiring new staff | 20 days | Mon 27/11/06 | Mon 25/12/06 |
| 74 | Implement defined implementation plan | 20 days | Mon 25/12/06 | Mon 22/01/07 |
| 75 | Implement procedures & processes | 20 days | Mon 22/01/07 | Mon 19/02/07 |
| 76 | Practice procedures & processes | 10 days | Mon 19/02/07 | Mon 05/03/07 |
| 77 | Plan CSIRT training courses | 2 days | Mon 05/03/07 | Wed 07/03/07 |
| 78 | Go operational | 0 hrs | Wed 07/03/07 | Wed 07/03/07 |

*Fig. 17 Project plan*



| ID | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 1 | **Concept phase (overall strategy)** | **17.5 days** | **Mon 14/08/06** | **Wed 06/09/06** |
| 2 | **Brainstorming** | **6.63 days** | **Mon 14/08/06** | **Tue 22/08/06** |
| 3 | Arrange brainstorming members | 4 days | Mon 14/08/06 | Thu 17/08/06 |
| 4 | Understanding what a CSIRT is | 1 hr | Fri 18/08/06 | Fri 18/08/06 |
| 5 | Defining the benefits of your CSIRT | 2 hrs | Fri 18/08/06 | Fri 18/08/06 |
| 6 | Defining your environment | 4 hrs | Fri 18/08/06 | Fri 18/08/06 |
| 7 | Defining the needs of your constituents | 4 hrs | Fri 18/08/06 | Mon 21/08/06 |
| 8 | Defining your intended services | 4 hrs | Mon 21/08/06 | Mon 21/08/06 |
| 9 | Defining the benefits of your CSIRT 02 | 2 hrs | Mon 21/08/06 | Tue 22/08/06 |
| 10 | Wrap up brainstorm | 0 hrs | Tue 22/08/06 | Tue 22/08/06 |
| 11 | **Communicating/Marketing approach** | **4.5 days** | **Mon 14/08/06** | **Fri 18/08/06** |
| 12 | Making a SWOT analysis | 1 day | Mon 14/08/06 | Mon 14/08/06 |
| 13 | Making a PEST analysis | 1 day | Tue 15/08/06 | Tue 15/08/06 |
| 14 | Choosing communication channels | 4 hrs | Wed 16/08/06 | Wed 16/08/06 |
| 15 | Draft your mission statement | 1 day | Wed 16/08/06 | Thu 17/08/06 |
| 16 | Wrap up outcome | 1 day | Thu 17/08/06 | Fri 18/08/06 |
| 17 | End of communication session | 0 hrs | Fri 18/08/06 | Fri 18/08/06 |
| 18 | **Documentation of Ideas** | **3.63 days** | **Fri 18/08/06** | **Wed 23/08/06** |
| 19 | Documentate brainstorm results | 1 day | Tue 22/08/06 | Wed 23/08/06 |
| 20 | Documentate Communication sessions | 1 day | Fri 18/08/06 | Mon 21/08/06 |
| 21 | Output documentated | 0 hrs | Mon 21/08/06 | Mon 21/08/06 |
| 22 | **Decision Workshop (mgt)** | **12 days** | **Mon 21/08/06** | **Wed 06/09/06** |
| 23 | Collecting business cases | 10 days | Mon 21/08/06 | Mon 04/09/06 |
| 24 | Collecting recent news articles | 10 days | Mon 21/08/06 | Mon 04/09/06 |
| 25 | Produce management presentation | 2 days | Mon 04/09/06 | Wed 06/09/06 |
| 26 | Plans accepted, go for developing impl. plan | 0 hrs | Wed 06/09/06 | Wed 06/09/06 |
| 27 | Kick-Off implementation phase | 0 hrs | Wed 06/09/06 | Wed 06/09/06 |
| 28 | **Preparatory implementation phase** | **41 days** | **Wed 06/09/06** | **Thu 02/11/06** |
| 29 | **Developing the Business Case** | **21 days** | **Wed 06/09/06** | **Thu 05/10/06** |
| 30 | Define your goals | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 31 | Define your CSIRT services | 8 days | Thu 07/09/06 | Tue 19/09/06 |
| 32 | Define your organizational structure | 8 days | Tue 19/09/06 | Fri 29/09/06 |
| 33 | Define the financial and revenue model | 4 days | Fri 29/09/06 | Thu 05/10/06 |
| 34 | Goals defined | 0 hrs | Thu 05/10/06 | Thu 05/10/06 |
| 35 | **Hiring the right staff** | **20 days** | **Thu 05/10/06** | **Thu 02/11/06** |
| 36 | Make job descriptions | 10 days | Thu 05/10/06 | Thu 19/10/06 |
| 37 | Hire staff | 10 days | Thu 19/10/06 | Thu 02/11/06 |
| 38 | Procedure started/people hired | 0 hrs | Thu 02/11/06 | Thu 02/11/06 |
| 39 | **Utilizing the CSIRT office** | **20 days** | **Wed 06/09/06** | **Wed 04/10/06** |
| 40 | Equipment | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 41 | Internet connectivity (or hosting) | 5 days | Wed 06/09/06 | Wed 13/09/06 |
| 42 | Website | 20 days | Wed 06/09/06 | Wed 04/10/06 |
| 43 | Plan CSIRT hosting | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 44 | **Record tracking systems** | **2 days** | **Wed 06/09/06** | **Fri 08/09/06** |
| 45 | CRM | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 46 | Incident ticket system | 1 day | Thu 07/09/06 | Fri 08/09/06 |
| 47 | Record tracking done | 0 hrs | Wed 06/09/06 | Wed 06/09/06 |
| 48 | **Communication systems** | **1 day** | **Wed 06/09/06** | **Thu 07/09/06** |
| 49 | Email facilities | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 50 | Telephone, Fax | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 51 | SMS | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 52 | Communication done | 0 hrs | Wed 06/09/06 | Wed 06/09/06 |
| 53 | Utilization office done | 0 hrs | Wed 04/10/06 | Wed 04/10/06 |
| 54 | **Developing the information Security policy** | **3 days** | **Wed 06/09/06** | **Mon 11/09/06** |
| 55 | Check compliancy with application law & legislatio | 1 day | Wed 06/09/06 | Thu 07/09/06 |
| 56 | Check compliancy with existing corp. policies | 1 day | Thu 07/09/06 | Fri 08/09/06 |
| 57 | Check policy on liability issues | 1 day | Fri 08/09/06 | Mon 11/09/06 |
| 58 | Compliancy & liability check done | 0 hrs | Mon 11/09/06 | Mon 11/09/06 |
| 59 | **Search for partners in the CSIRT workfield** | **4 days** | **Wed 06/09/06** | **Tue 12/09/06** |
| 60 | Check TF-CSIRT membership | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 61 | Check FIRST-membership | 4 days | Wed 06/09/06 | Tue 12/09/06 |
| 62 | Check ENISA website | 2 days | Wed 06/09/06 | Fri 08/09/06 |
| 63 | Search done | 0 hrs | Tue 12/09/06 | Tue 12/09/06 |
| 64 | **Search for pilot customers** | **10 days** | **Wed 06/09/06** | **Wed 20/09/06** |
| 65 | Ask for input about the basic & services | 10 days | Wed 06/09/06 | Wed 20/09/06 |
| 66 | Accepted pilot customers | 0 hrs | Wed 20/09/06 | Wed 20/09/06 |
| 67 | Preparation done | 0 hrs | Thu 02/11/06 | Thu 02/11/06 |
| 68 | **Implementation phase** | **85 days** | **Thu 02/11/06** | **Wed 07/03/07** |
| 69 | Answer business case questions | 2 days | Thu 02/11/06 | Mon 06/11/06 |
| 70 | Define business plan | 5 days | Mon 06/11/06 | Mon 13/11/06 |
| 71 | Get approval of business case and budget | 10 days | Mon 13/11/06 | Mon 27/11/06 |
| 72 | Final go from management | 0 hrs | Mon 27/11/06 | Mon 27/11/06 |
| 73 | Hiring new staff | 20 days | Mon 27/11/06 | Mon 25/12/06 |
| 74 | Implement defined implementation plan | 20 days | Mon 25/12/06 | Mon 22/01/07 |
| 75 | Implement procedures & processes | 20 days | Mon 22/01/07 | Mon 19/02/07 |
| 76 | Practice procedures & processes | 10 days | Mon 19/02/07 | Mon 05/03/07 |
| 77 | Plan CSIRT training courses | 2 days | Mon 05/03/07 | Wed 07/03/07 |
| 78 | Go operational | 0 hrs | Wed 07/03/07 | Wed 07/03/07 |

*Fig. 18 The project plan with all tasks and a part of the Gant chart*

The project plan also is available in CVS- and XML-format. Further utilisation can be requested from ENISAs CSIRT experts:

CERT-Relations@enisa.europa.eu

# APPENDIX

## A.1 Further reading

**Handbook for CSIRTs (CERT/CC)**
A very comprehensive work of reference for all topics relevant for the work of a CSIRT
Source: http://www.cert.org/archive/pdf/csirt-handbook.pdf

**Defining Incident Management Processes for CSIRTs: A Work in Progress**
An in-depth analysis of incident management
Source: http://www.cert.org/archive/pdf/04tr015.pdf

**State of the Practice of Computer Security Incident Response Teams (CSIRTs)**
A comprehensive analysis of the actual situation concerning the world-wide CSIRT landscape, including history, statistics and much more
Source: http://www.cert.org/archive/pdf/03tr001.pdf

**CERT-in-a-box**
A comprehensive description of the lessons learned from setting up GOVCERT.NL and 'De Waarschuwingsdienst', the Dutch national Alerting service.
Source: http://www.govcert.nl/render.html?it=69

**RFC 2350: Expectations for Computer Security Incident Response**
Source: http://www.ietf.org/rfc/rfc2350.txt

**NIST[37] Computer Security Incident Handling Guide**
Source: http://www.securityunit.com/publications/sp800-61.pdf

**ENISA Inventory of CERT activities in Europe**
A work of reference that lists information about CSIRTs in Europe and their various activities
Source: http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] NIST: National Institute of Standards and Technologies

## A.2 CSIRT Services

A special thanks to CERT/CC, who provided this list

| ***Reactive Services*** | ***Proactive Services*** | ***Artifact Handling*** |
|---|---|---|
| • Alerts and Warnings<br>• Incident Handling<br>• Incident analysis<br>• Incident response on site<br>• Incident response support<br>• Incident response coordination<br>• Vulnerability Handling<br>• Vulnerability analysis<br>• Vulnerability response<br>• Vulnerability response coordination | • Announcements<br>• Technology Watch<br>• Security Audits or Assessments<br>• Configuration and Maintenance of Security<br>• Development of Security Tools<br>• Intrusion Detection Services<br>• Security-Related Information Dissemination | • Artifact analysis<br>• Artifact response<br>• Artifact response coordination<br>***Security Quality Management***<br>• Risk Analysis<br>• Business Continuity and Disaster Recovery<br>• Security Consulting<br>• Awareness Building<br>• Education/Training<br>• Product Evaluation or Certification |

*Fig. 19 CSIRT Services list from CERT/CC*

### Service Descriptions

### Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

### Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

### Incident Handling

Incident handling involves receiving, triaging and responding to requests and reports, and analysing incidents and events. Particular response activities can include

- taking action to protect systems and networks affected or threatened by intruder activity
- providing solutions and mitigation strategies from relevant advisories or alerts
- looking for intruder activity on other parts of the network

- filtering network traffic
- rebuilding systems
- patching or repairing systems
- developing other response or workaround strategies

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

**Incident analysis**

There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are

**Forensic evidence collection**

The collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.

**Tracking or tracing**

The tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organisations.

### Incident response on site

The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyses the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.

### Incident response support

The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

### Incident response coordination

The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organisation's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

### Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities; analysing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

### Vulnerability analysis

The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

### Vulnerability response

This service involves determining the appropriate response to mitigate or repair vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts. This service can include performing the response by installing patches, fixes, or workarounds.

### Vulnerability response coordination

The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesising technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledgebase of vulnerability information and corresponding response strategies.

### Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorised or disruptive activities. Once received, the artifact is reviewed. This includes analysing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorised based on the type of activities performed and the type of assistance given as follows:

### Artifact analysis

The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

### Artifact response

This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

### Artifact response coordination

This service involves sharing and synthesising analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesising technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

### Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

### Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

### Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

### Security Audits or Assessments

This service provides a detailed review and analysis of an organisation's security infrastructure, based on the requirements defined by the organisation or by other industry standards that apply. It can also involve a review of the organisational security practices. There are many different types of audits or assessments that can be provided, including

### Infrastructure review

Manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organisational or industry best practice security policies and standard configurations

### Best practice review

Interviewing employees and system and network administrators to determine if their security practices match the defined organisational security policy or some specific industry standards

### Scanning

Using vulnerability or virus scanners to determine which systems and networks are vulnerable.

### Penetration testing

Testing the security of a site by purposefully attacking its systems and networks
Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organisational policy. Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

### Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

### Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customised software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

### Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyse and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analysing the large amounts of data captured. In many cases, specialised tools or expertise is required to synthesise and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimise such events. Some organisations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

### Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links
- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organisation (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

### Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organisation. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organisation. Depending on organisational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organisational team effort.

The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

### Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organisation's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

### Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

### Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organisational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

### Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organisational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimising losses.

CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organisational systems.

### Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

### Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organisational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organisation or by the CSIRT.

## A.3 The examples

**Fictitious CSIRT**

**Step 0 - Understanding what a CSIRT is:**

The sample CSIRT will have to serve a medium institution made up of 200 staff members. The institution has its own IT department and two other branch offices in the same country. IT plays a key roll for the company because it's used for internal communication, data network and a 24x7 e-business. The institution has its own network and disposes of a redundant connection to the internet via two different ISPs.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Step 1: Starting phase**

In the starting phase the new CSIRT is planned as an Internal CSIRT, providing its services for the hosting company the local IT department and the staff. It also supports and coordinates the handling of IT security related incidents between the different branch offices.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Step 2: Choosing the right services**

In the starting phase it is decided that the new CSIRT will focus mainly on providing some of the core-services for the employees.

It's decided that after a pilot-phase the extension of the service portfolio might be considered and Security Management Services might be added. That decision will be made based on the feedback from the pilot-constituents and in close cooperation with the Quality Assurance department.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Step 3: Making an analysis of the constituency and the appropriate communication channels**

A brainstorming session with some key persons from management and the constituency generated enough input for a SWOT analysis. This lead to the conclusion that there is a need for the core-services:

- Alerts and warnings
- Incident handling (analysis, response support and response coordination)
- Announcements

It must be ensured that the information is distributed in a well-organised manner to reach a biggest possible part of the constituency. So the decision is made that alerts, warnings and announcements in the form of security advisories will be published on a dedicated website and distributed via a mailing list. The CSIRT facilitates e-mail, phone and fax for receiving of incident reports. A unified web-form is planned for the next step.

**Step 4: Mission Statement**

The management of the fictitious CSIRT has made the following mission statement:
*“Fictitious CSIRT provides information and assistance to the staff of its hosting company to reduce the risks of computer security incidents as well as responding to such incidents when they occur.”*

By this fictitious CSIRT makes clear that it is an internal CSIRT and that its core business is to deal with IT security related issues.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Step 5: Defining the Business Plan**

**Financial model**
Due to the fact that the company has 24x7 e-business and also a 24x7 IT department it’s decided to provide full service during office hours and an on call duty for outside office hours. The services for the constituency will be provided for free, but the possibility to deliver services for external customers will be assessed during the pilot- and evaluation phase.

**Revenue model**
During the starting- and pilot-phase the CSIRT will be financed through the hosting company. During the pilot- and the evaluation phase additional funding will be discussed, including the possibility to sell services to external customers.

**Organisational model**
The hosting organisation is a small company, so the embedded model is chosen.
During office hour a staff of three people will provide the core-services (distribution of security advisories and incident handling/coordination).

The company’s IT department already employs people with suitable skills. An agreement with that department is made so that the new CSIRT can request support on an ad-hoc basis when needed. Also the 2nd line of their on-call technicians can be used.
There will be a core CSIRT team with four full-time members and five additional CSIRT team members. One of those is also available on circulating shift.

**Staff**
The CSIRT team leader has a background in security and 1st and 2nd level support and has done work in the resilience crisis management work field. The other three team members are security specialists. The part-time CSIRT team members from the IT department are specialists on their part of the company’s infrastructure.

### Step 5 Utilising the office and information security policy

### Office equipment and location

Due to the fact that the hosting company already has efficient physical security in place, the new CSIRT is well covered in that aspect. A so called “war room” is provided for enabling coordination in the case of an emergency. A safe is purchased for the encryption material and sensitive documents. A separate telephone line was established including a switchboard for facilitating the hotline during office hours and the “on-call” duty mobile phone for the time outside office hours with the same phone number.

Existing equipment and the corporate website to announce CSIRT related information can also be used. A mailing list software is installed and maintained, with a restricted part for the communication among team members and with other teams. All contact detail of the staff members is stored in a database; a print-out is kept in the safe.

### Regulation

Due to the fact that the CSIRT is embedded in a company with existing information security policies the according policies for the CSIRT have been established with the help of the legal adviser of the company.

- - - - - - - - - - - - - - - - - - - - - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -

### Step 7 Looking for cooperation

By using ENISAs Inventory quickly some CSIRTs in the same country could have been found and contacted. A site visit was arranged with one of them for the newly hired team leader. He learned about national CSIRT activity and attended a meeting.
This meeting was more than helpful for collecting examples of working methods and get support by a couple of other teams.- - - - - - - - - - - - - - - - - - - - - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -

### Step 8 Promoting the Business Plan

It’s decided to collect facts and figures from the company’s history. This is more than useful for a statistical overview of the IT security situation. This collection should be continued when the CSIRT is up and running, to keep the statistics up-to-date.

Other national CSIRTs were contacted and interviewed about their business cases. They provided support by compiling some slides with information about recent developments in IT security incidents and about costs of incidents.

In this example case of fictious CSIRT there was no pressing need to convince the management about the importance of IT business, and so it was not hard to get the go-ahead for the first step. A business case and a project plan where prepared, including an estimation of the set-up costs and the cost of operation.

- - - - - - - - - - - - - - - - - - - - - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -

**Step 9 Establishing process flows and operational and technical procedures**
Fictious CSIRT focuses on delivering core CSIRT services:

- Alerts and Warnings
- Announcements
- Incident Handling

The team developed procedures that work well and that are easily understandable by every team member. Fictious CSIRT also hired a legal expert to deal with liabilities and the information security policy. The team adopted some useful tools and found helpful information about operational issues by discussing with other CSIRTs.

A fixed template for security advisories and incident reports was generated. The team uses RTIR for incident handling.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

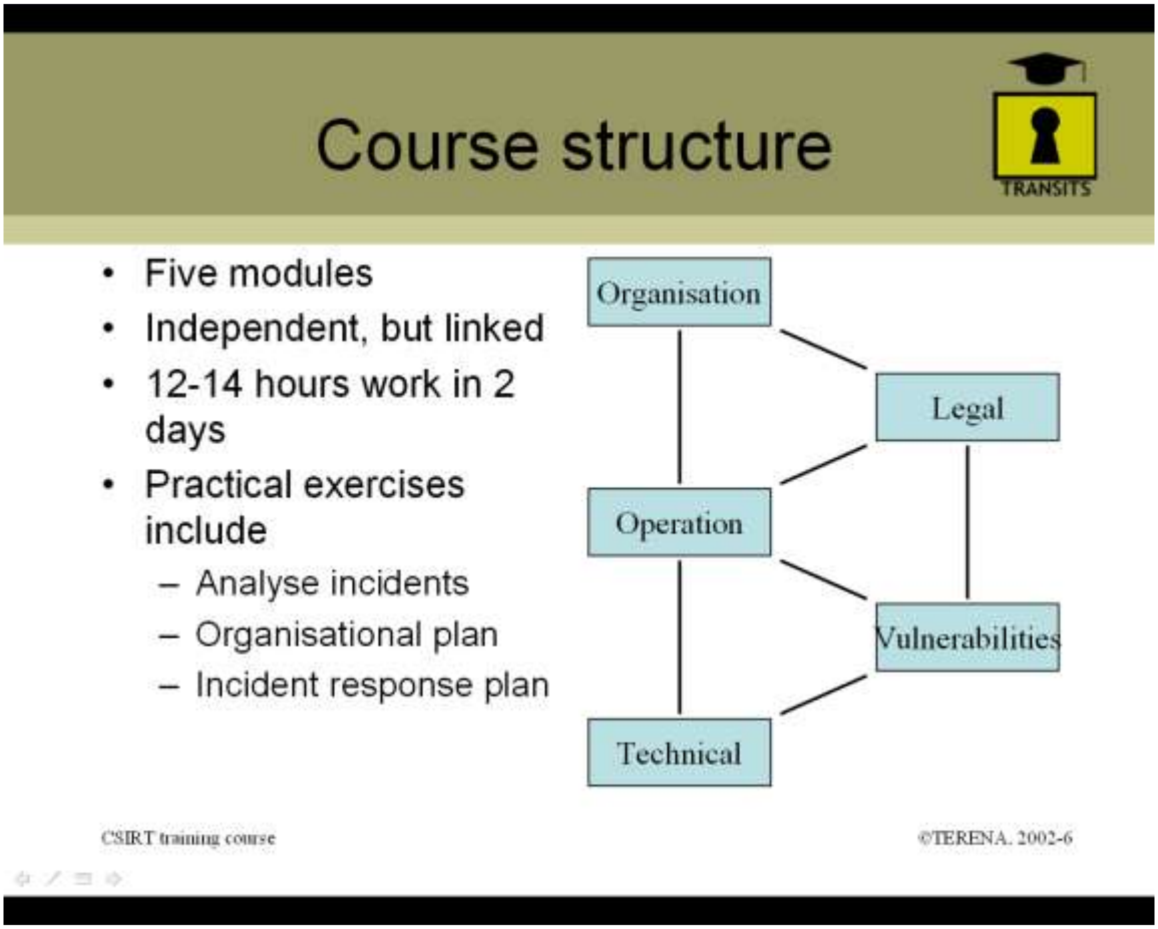
**Step 10 Training the staff**
Fictious CSIRT decides to send all their technical staff to the next available TRANSITS courses. The team leader additionally attends the *Managing a CSIRT* course from CERT/CC.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Step 11: Exercising**
During the first weeks of operations fictious CSIRT used several fictious cases (that they got as examples from other CSIRTs) that where used as exercise. Furthermore they issued a couple of security advisories based on real vulnerability information distributed by hard- and software vendors, that they fine-tuned and adjusted to the needs of the constituency.

## A.4 Sample Material from CSIRT Courses

**TRANSITS (With kind permission of Terena, http://www.terena.nl)**



Course structure

- Five modules
- Independent, but linked
- 12-14 hours work in 2 days
- Practical exercises include
  - Analyse incidents
  - Organisational plan
  - Incident response plan

Organisation

Legal

Operation

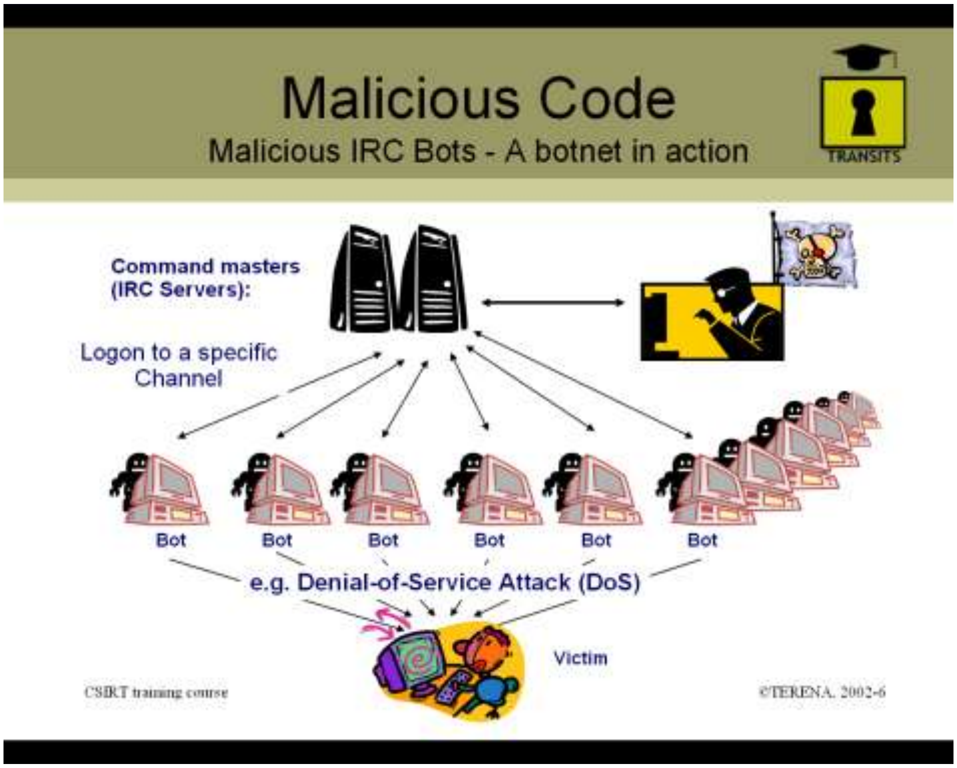
Vulnerabilities

Technical

CSIRT training course

©TERENA, 2002-6

Overview: The course structure



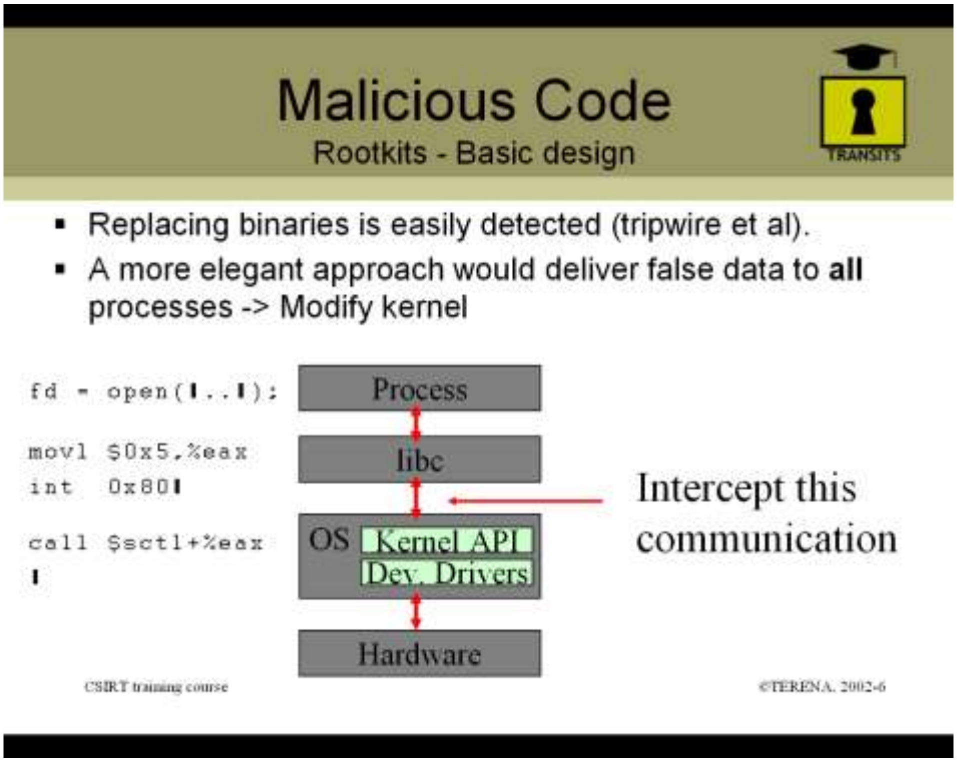
## Malicious Code

Malicious IRC Bots - A botnet in action

CSIRT training course

©TERENA, 2002-6

From the *Technical module*: Description of a Botnet



## Malicious Code

Rootkits - Basic design

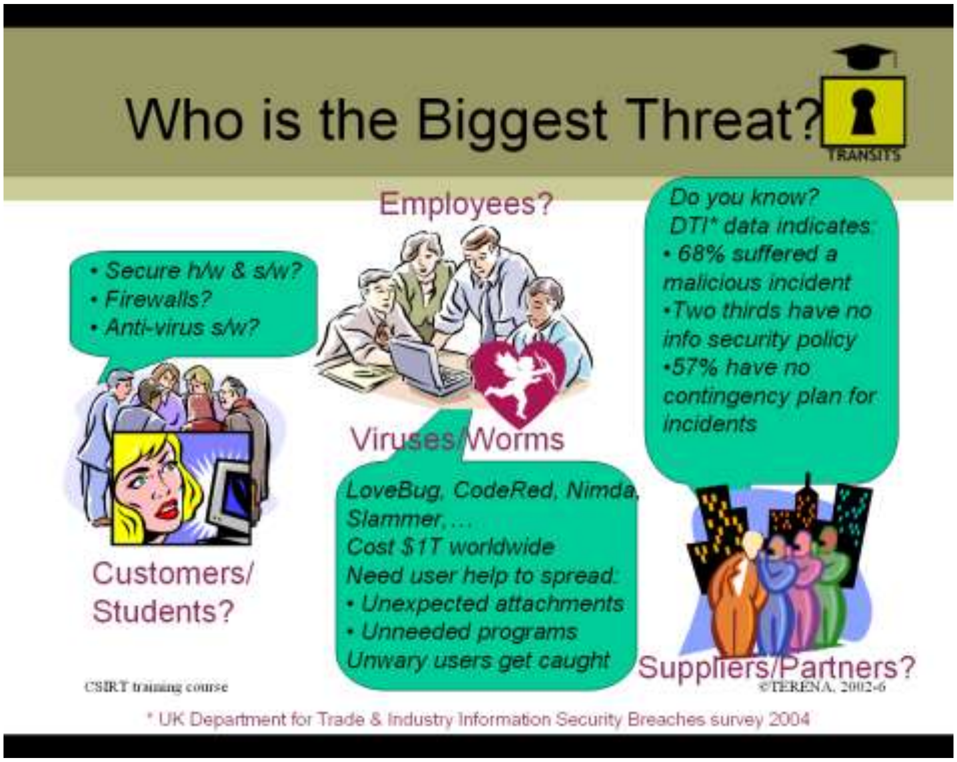
- Replacing binaries is easily detected (tripwire et al).
- A more elegant approach would deliver false data to **all** processes -> Modify kernel

```
fd = open(▮..▮);

movl $0x5,%eax
int  0x80▮

call $sctl+%eax
▮
```

CSIRT training course

©TERENA, 2002-6

From the *Technical module*: Basic design of a rootkit



## Who is the Biggest Threat?

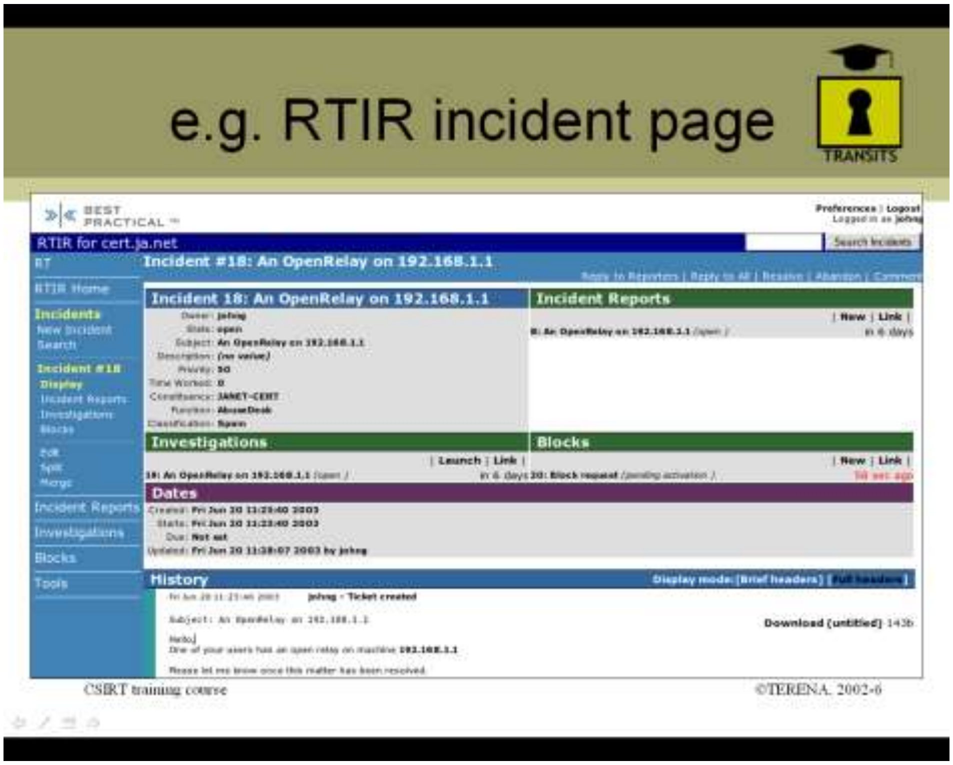
Do you know?
DTI* data indicates:
• 68% suffered a malicious incident
•Two thirds have no info security policy
•57% have no contingency plan for incidents

LoveBug, CodeRed, Nimda, Slammer, …
Cost $1T worldwide
Need user help to spread:
• Unexpected attachments
• Unneeded programs
Unwary users get caught

CSIRT training course ©TERENA, 2002-6

* UK Department for Trade & Industry Information Security Breaches survey 2004

From the *Organisational module*: Insider or outsider – where is the bigger threat?



## e.g. RTIR incident page

Incident #18: An OpenRelay on 192.168.1.1

Incident 18: An OpenRelay on 192.168.1.1

Owner: johng
State: open
Subject: An OpenRelay on 192.168.1.1
Description: (no value)
Priority: 50
Time Worked: 0
Constituency: JANET-CERT
Function: AbuseDesk
Classification: Spam

Incident Reports

8: An OpenRelay on 192.168.1.1 (open) in 6 days

Investigations

18: An OpenRelay on 192.168.1.1 (open) in 6 days

Blocks

20: Block request (pending activation) 58 sec ago

Dates

Created: Fri Jun 20 11:23:40 2003
Starts: Fri Jun 20 11:23:40 2003
Due: Not set
Updated: Fri Jun 20 11:38:07 2003 by johng

History

Fri Jun 20 11:23:40 2003 johng - Ticket created

Subject: An OpenRelay on 192.168.1.1

Download (untitled) 143b

Hello,
One of your users has an open relay on machine 192.168.1.1

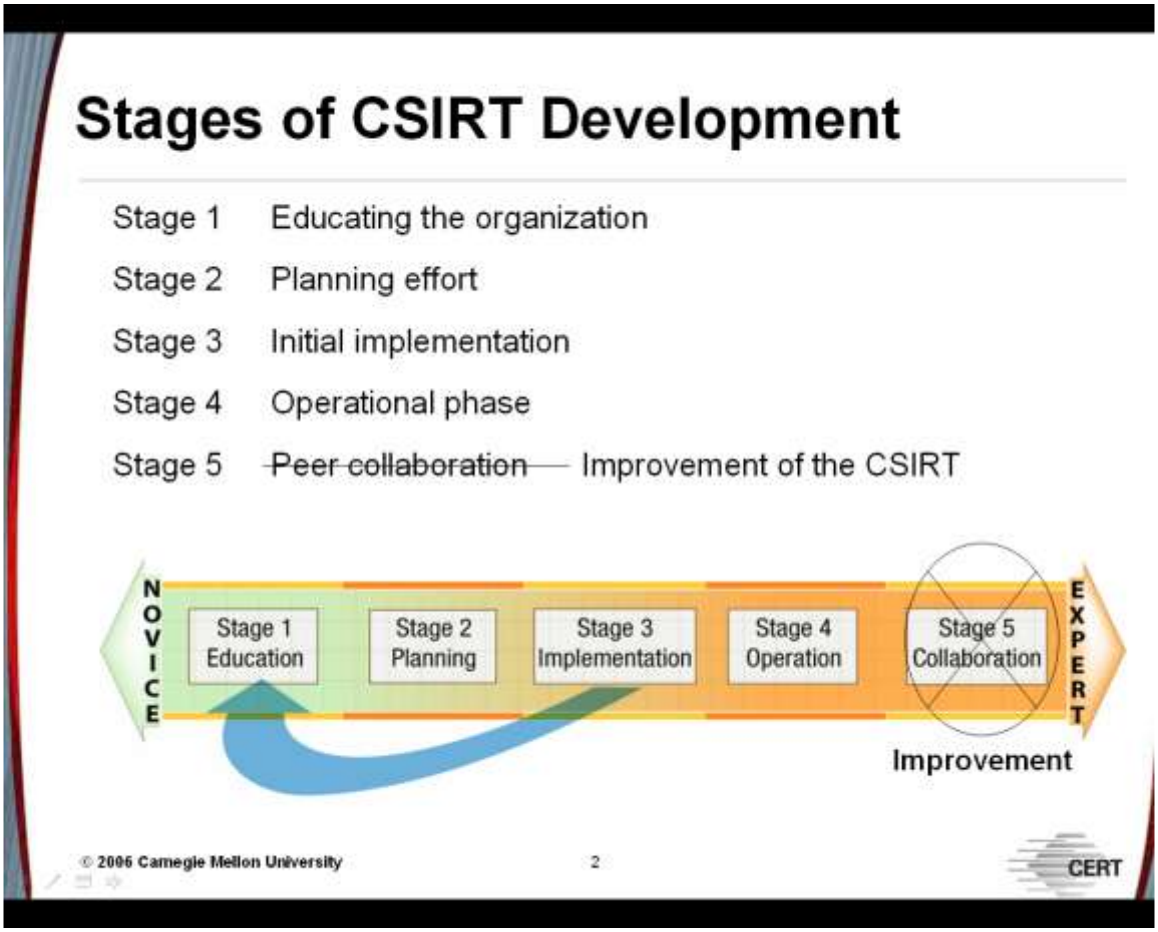
Please let me know once this matter has been resolved.

CSIRT training course ©TERENA, 2002-6

From the *Operational track*: Request Tracker for Incident Response (RTIR)

**“Setting up of CSIRTs” (with kind permission from CERT/CC, http://www.cert.org )**

***ENISA gratefully acknowledges the CSIRT Development Team at the CERT Program for allowing us the use of content from their training courses!***

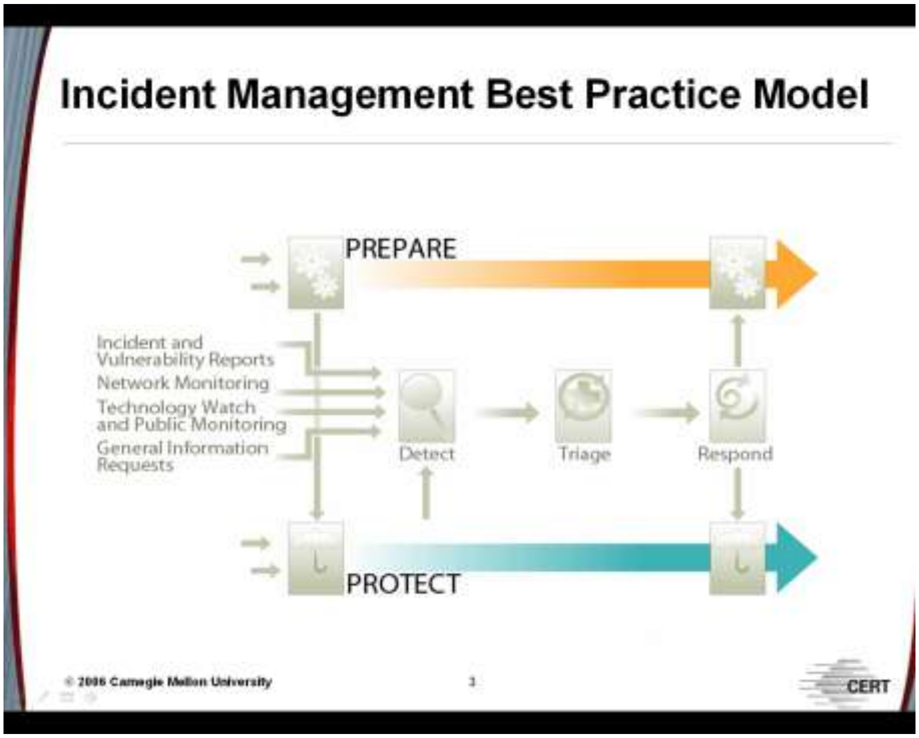


## Stages of CSIRT Development

| | |
|---|---|
| Stage 1 | Educating the organization |
| Stage 2 | Planning effort |
| Stage 3 | Initial implementation |
| Stage 4 | Operational phase |
| Stage 5 | ~~Peer collaboration~~ — Improvement of the CSIRT |

© 2006 Carnegie Mellon University 2 CERT

From *CERT/CC Training course*: Stages of CSIRT development



## Incident Management Best Practice Model

PREPARE

Incident and Vulnerability Reports

Network Monitoring

Technology Watch and Public Monitoring

General Information Requests

Detect

Triage

Respond

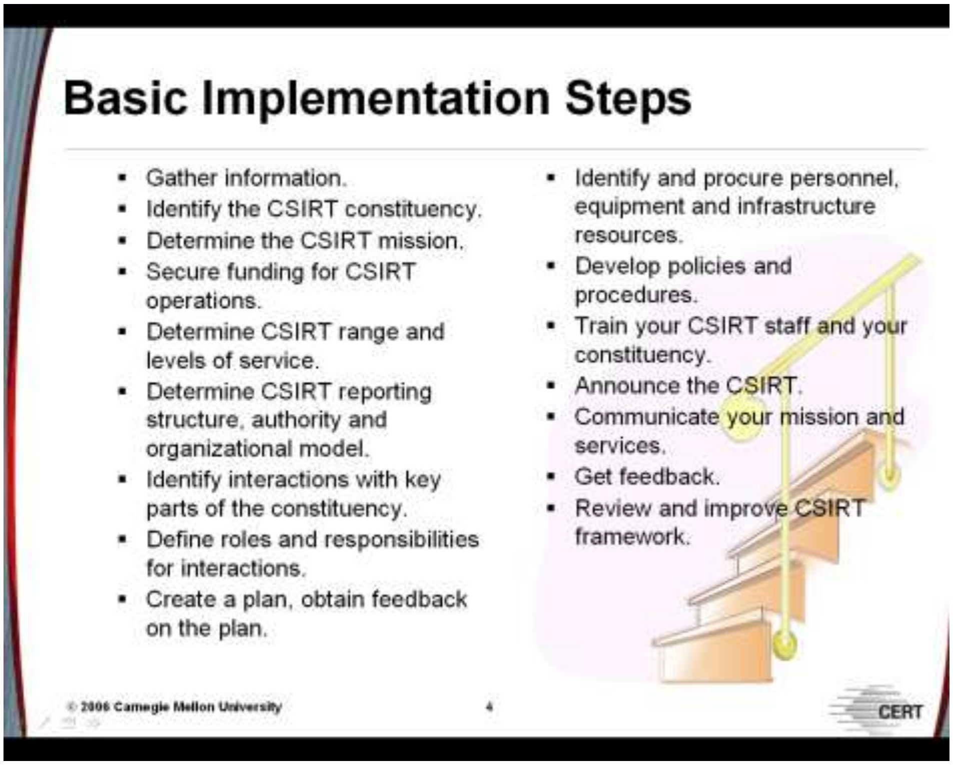
PROTECT

© 2006 Carnegie Mellon University

3

CERT

From *CERT/CC Training course*: Best practice in incident management



## Basic Implementation Steps

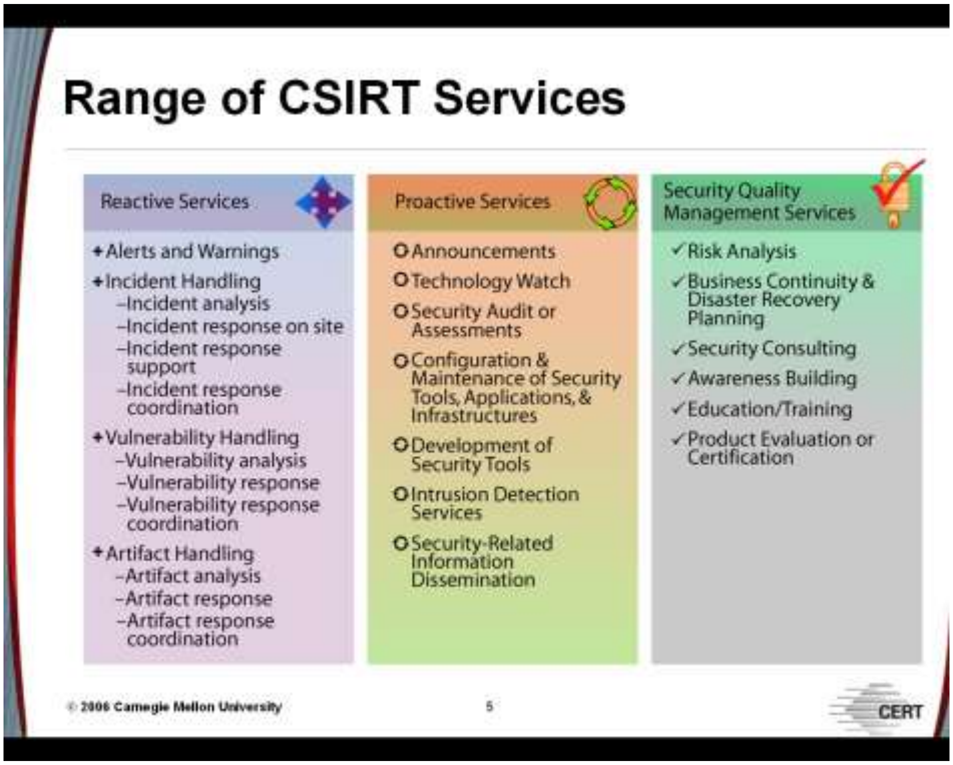
- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and improve CSIRT framework.

© 2006 Carnegie Mellon University

4

CERT

From *CERT/CC Training course*: Steps to follow when setting up a CSIRT



## Range of CSIRT Services

**Reactive Services**

- ✦ Alerts and Warnings
- ✦ Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- ✦ Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- ✦ Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

**Proactive Services**

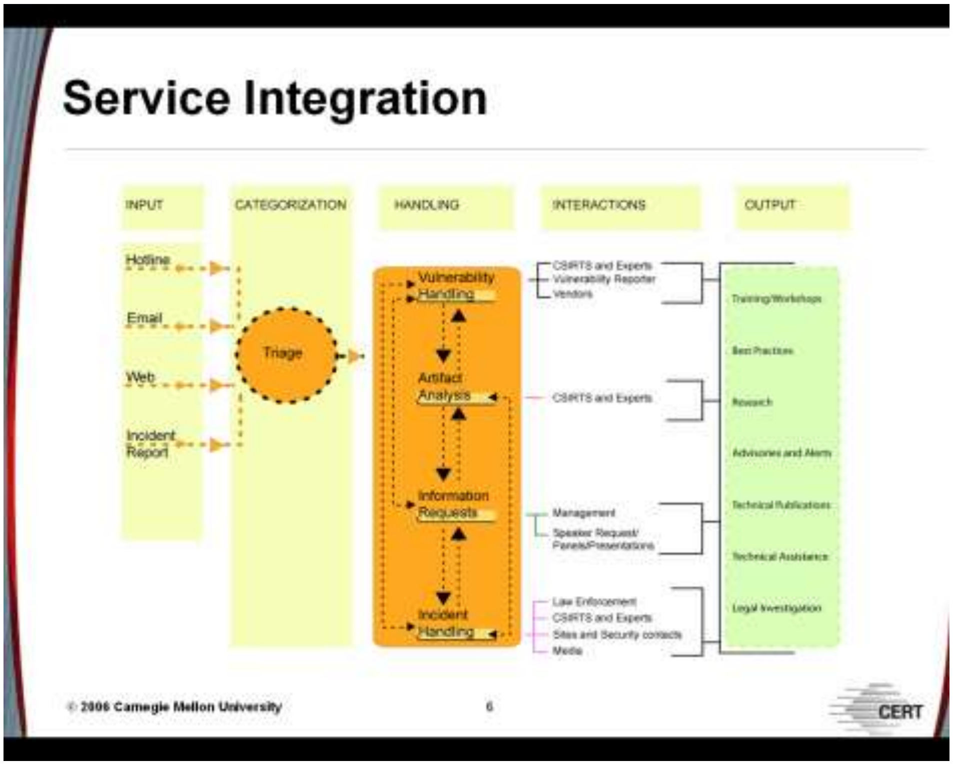
- ○ Announcements
- ○ Technology Watch
- ○ Security Audit or Assessments
- ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ○ Development of Security Tools
- ○ Intrusion Detection Services
- ○ Security-Related Information Dissemination

**Security Quality Management Services**

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

© 2006 Carnegie Mellon University 5 CERT

From *CERT/CC Training course:* The services a CSIRT can provide



## Service Integration

INPUT

Hotline

Email

Web

Incident Report

CATEGORIZATION

Triage

HANDLING

Vulnerability Handling

Artifact Analysis

Information Requests

Incident Handling

INTERACTIONS

CSIRTS and Experts

Vulnerability Reporter

Vendors

CSIRTS and Experts

Management

Speaker Request/ Panels/Presentations

Law Enforcement

CSIRTS and Experts

Sites and Security contacts

Media

OUTPUT

Training/Workshops

Best Practices

Research

Advisories and Alerts

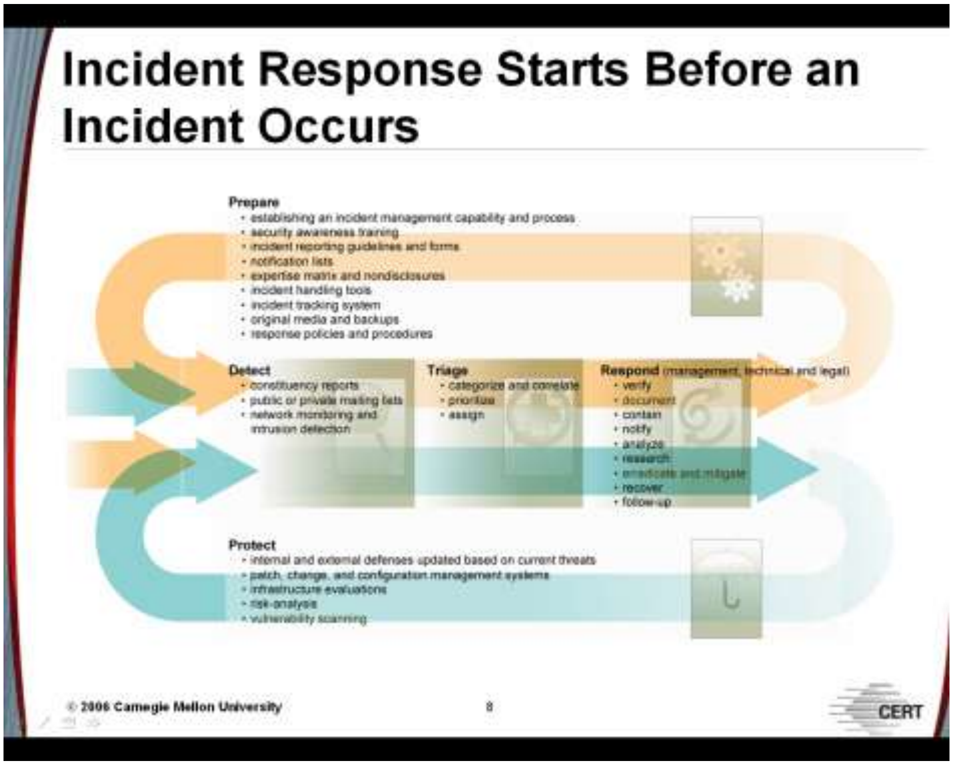
Technical Publications

Technical Assistance

Legal Investigation

© 2006 Carnegie Mellon University 6 CERT

From *CERT/CC Training course:* The incident management workflow



## Incident Response Starts Before an Incident Occurs

**Prepare**
- establishing an incident management capability and process
- security awareness training
- incident reporting guidelines and forms
- notification lists
- expertise matrix and nondisclosures
- incident handling tools
- incident tracking system
- original media and backups
- response policies and procedures

**Detect**
- constituency reports
- public or private mailing lists
- network monitoring and intrusion detection

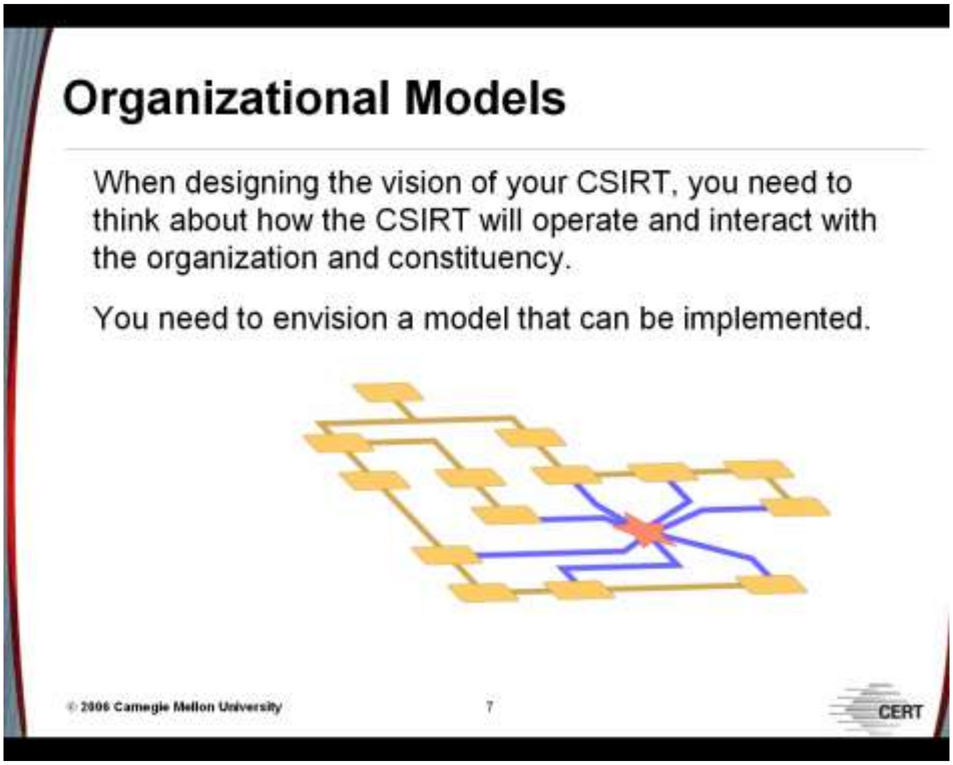
**Triage**
- categorize and correlate
- prioritize
- assign

**Respond** (management, technical and legal)
- verify
- document
- contain
- notify
- analyze
- research
- eradicate and mitigate
- recover
- follow-up

**Protect**
- internal and external defenses updated based on current threats
- patch, change, and configuration management systems
- infrastructure evaluations
- risk-analysis
- vulnerability scanning

© 2006 Carnegie Mellon University 8 CERT

From *CERT/CC Training course:* Incident response



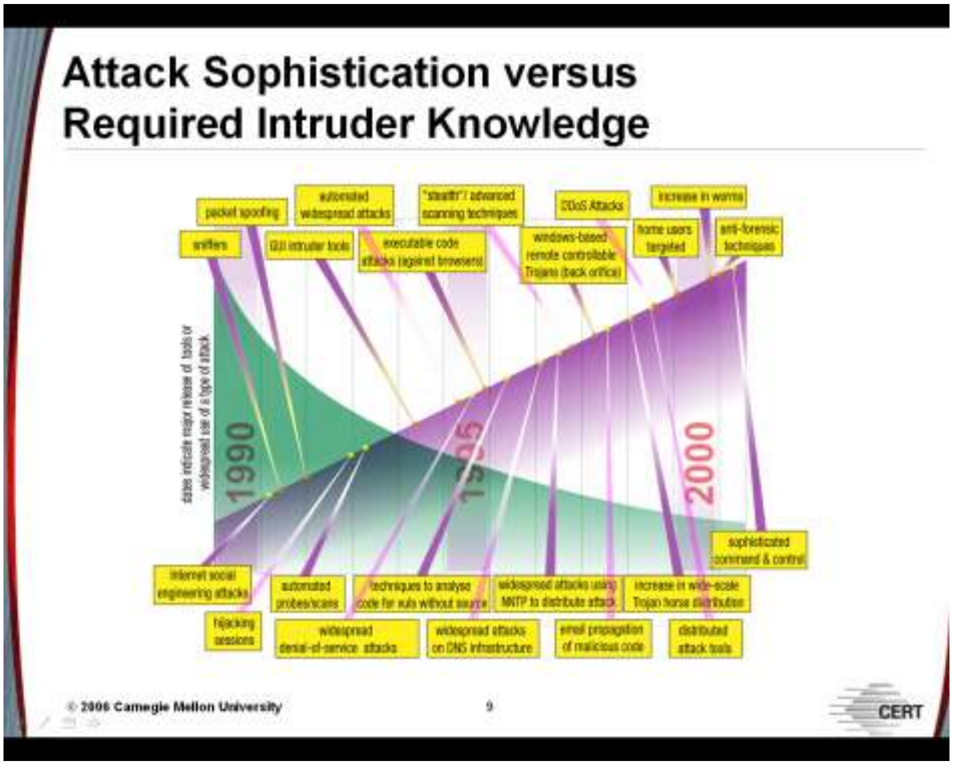
## Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

You need to envision a model that can be implemented.

© 2006 Carnegie Mellon University 7 CERT

From *CERT/CC Training course:* How will the CSIRT be organised?



Attack Sophistication versus Required Intruder Knowledge

© 2006 Carnegie Mellon University 9

CERT

From *CERT/CC Training course:* Less knowledge, more damage